IN THE

𝔘𝔫𝔦𝔱𝔢𝔡 𝔖𝔱𝔞𝔱𝔢𝔰 𝔠𝔬𝔲𝔯𝔱 𝔬𝔣 𝔄𝔭𝔭𝔢𝔞𝔩𝔰
𝔣𝔬𝔯 𝔱𝔥𝔢 𝔇𝔦𝔰𝔱𝔯𝔦𝔠𝔱 𝔬𝔣 ℭ𝔬𝔩𝔲𝔪𝔟𝔦𝔞 ℭ𝔦𝔯𝔠𝔲𝔦𝔱

—————————

TIKTOK INC. and BYTEDANCE LTD.

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

—————————

caption continued on inside cover

—————————

On Petitions for Review of Constitutionality of
the Protecting Americans from Foreign Adversary Controlled
Applications Act

—————————

**APPENDIX TO BRIEF OF PETITIONERS
TIKTOK INC. AND BYTEDANCE LTD.
Volume II of III (Pages 261–529)**

—————————

Andrew J. Pincus
Avi M. Kupfer
MAYER BROWN LLP
1999 K Street, NW
Washington, DC 20006
(202) 263-3220
apincus@mayerbrown.com

*Counsel for Petitioners
TikTok Inc. and ByteDance Ltd.
(continued on inside cover)*

Alexander A. Berengaut
 Counsel of Record
David M. Zionts
Megan A. Crowley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
aberengaut@cov.com

BRIAN FIREBAUGH et al.,

Petitioners,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

_____

BASED Politics Inc.,

Petitioner,

v.

MERRICK B. GARLAND, in his official capacity as Attorney General of the United States,

Respondent.

John E. Hall
Anders Linderot
S. Conrad Scott
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, New York 10018
(212) 841-1000

Counsel for Petitioners
TikTok Inc. and ByteDance Ltd.

TABLE OF CONTENTS

Volume I

Volume II

Volume III

Declaration of Alexander A. Berengaut (continued)

iv

Exhibit C

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States
September 17, 2021

ByteDance Participants

- **Erich Andersen** – General Counsel and Head of Corporate Affairs
- **Vanessa Pappas** (telephonic) – TikTok Chief Operating Officer
- **Will Farrell** – TikTok Head of Global Cyber and Data Defense
- **Matt Penarczyk** – TikTok Head of Legal, Americas
- **Sarah Aleem** – TikTok Senior Legal Counsel, North America

Oracle Participants (telephonic)

- **Edward Screven** – Chief Corporate Architect
- **Craig Stephen** – Senior Vice President, Research and Development
- **Scott Gaetjen** – Vice President, Cloud Chief Architect
- **Brian Higgins** – Senior Vice President, Legal

Counsel

- **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **B.J. Altvater** (Covington) on behalf of ByteDance
- **Giovanna Cinelli** and **Christian Kozlowski** from Morgan Lewis on behalf of Oracle

APP-262

Topics for Today's Discussion

1	Key objectives in designing the governance model for TikTok operations in the United States
2	Overview of proposed governance model for TikTok operations in the United States
3	Conclusions and Q&A

APP-263

Key Governance Objectives

Safeguard Protected Data, provide software assurance, and defend against malign foreign influence (together, the "National Security Functions").

Maintain a global, interoperable short-form video platform business that ensures continued consistency between U.S. and non-U.S. user experiences.

Implement an operationally feasible agreement that has robust, sustainable compliance and oversight functions as the business evolves.

APP-264

Development of Governance Model

Questions Presented	Key Considerations
How do we secure the U.S. National Security Functions for a global platform?	• Identify U.S. user data and who needs access to it • Deploy ByteDance software code securely for the app and back-end • Provide day-to-day operation of the platform • Understand and address national security concerns related to content *Must identify the right resources, management, and partners to accomplish all of the foregoing.*
How can we secure the National Security Functions without breaking the business in and outside the United States?	• Streamline Non-National Security Functions across a globally integrated platform • Protect intellectual property developed by ByteDance that drives the platform • Satisfy duty to shareholders, who are predominantly Western/non-Chinese, to maintain profitability and growth *To accomplish the foregoing requires talented, experienced management; experience with TikTok itself and its technologies; and clear alignment in business objectives and incentives.*
How can the model comply with global regulatory requirements?	• TikTok is a global business that must have a sustainable governance and operational model that also can fit with legal and regulatory requirements in other countries, including Chinese export control restrictions *The solution must be one that considers holistically the impact on the business and operations in the U.S. and abroad, and to the extent possible anticipates future regulatory developments.*

APP-265

Development of Governance Model

Conclusions from in-depth planning exercise driven by the foregoing considerations:

1	National Security Functions should be in a special security organization that has fully independent governance of said functions, with TTP and third-party monitoring to provide additional protections
2	Enable the business facing functions to remain globally integrated with current management
3	Build alignment by identifying the right management for TikTok U.S. Ops, having BD minority board representation on TikTok U.S. Ops, and providing for clear operating principles on certain business management and planning tools (*e.g.*, budget, performance metrics)

*ByteDance has undertaken an intense effort to build the governance model
– and build out TikTok U.S. Ops – based on these principles.*

APP-266

Challenges with Governance at TikTok Inc.

Objective	TikTok Inc.
Secure National Security Functions	• TikTok Inc. manages aspects of its business well-beyond the National Security Functions; wrapping all the mitigation under TikTok Inc. is unnecessary and overbroad and would be significantly harder to operationalize and monitor. • Focusing the operation of the National Security Functions in TikTok U.S. Ops ensures high level of focus and operational control.
Preserve interoperability for Global Business with respect to Non-National Security Functions	• High risk of "breaking the business" through excessive segregation of the U.S. operations from the rest of the world, and interjection of outsiders who lack the requisite experience and background to manage and operate a hugely complex and inherently global social media business. • Core non-National Security Functions for the U.S. market can not be disentangled from the global business and integration would not be possible under a independent governance at TikTok Inc.– instead, the business would effectively be operated in a silo and separated from the rest of the world.
Comply with Global Regulatory Requirements	• If ByteDance is rendered to a minority position or passive over the entire U.S. business, it will not be able to secure the necessary authorizations from Chinese regulators. • Further, a change of control for Rest of World operations could trigger regulatory review in other jurisdictions.

Proposed Governance Model

We believe the following governance structure will resolve national security concerns while also preserving TikTok's global presence.

Shareholder: TikTok Inc.

ByteDance Ltd.

ByteDance POC

TikTok Inc.

Compliance Officer

TikTok U.S. Ops Board *Directors*

ByteDance Director

ByteDance Director

Security Director / Chair of the Board

Security Director / Chair of Compliance Committee

Security Director

Oracle

Trusted Technology Provider

Technology Officer

No National Security Responsibility

Full National Security Responsibility

Indicates communication with CFIUS Monitoring Agencies

TikTok U.S. Ops
Security Officer

Content Advisory Council

Third Party Auditor

Third Party Monitor

CFIUS Monitoring Agencies *(with Review & Inspection Rights)*

APP-268

TikTok U.S. Ops Functions

To segregate these National Security Functions, TikTok U.S. Ops will need to transfer and hire approximately 1,500 personnel before it is operational; this number will continue to grow over time given the scale of the business.

TikTok U.S. Ops
Head of TikTok U.S. Ops

Subset of Product & RD	**Ads Integrity**	**Subset of Security**	**U.S. Operations**	**U.S. Trust & Safety**	**Legal & Compliance**	**Human Resources**	**General Services**	**Finance**
Requires access to PD for: -Infrastructure -Platform -Product *Includes Monetization Product	Requires access to PD for: -Ads integrity -Model training -Fraud detection	Requires access to PD for: -CIB Defense -Threat detection & response -Data protection -Security & Privacy Compliance	Requires access to PD for: -User Support -Product Operations -Tools & Reporting -Insights & Analytics	Requires access to PD for: -Safety Operations -Risk Models -Strategy and analytics -Law Enforcement	Support for - Compliance obligations -Employment support	Support for -Implementing people philosophy -Making key people decisions	Support for administrative and support teams including: -IT services, -Admin services, -Real estate and facilities	Support for -Revenue and cash management -Accounting -Tax -Financial planning and analysis
Est. Head Count = 375	**Est. Head Count = 15**	**Est. Head Count = 150**	**Est. Head Count = 375**	**Est. Head Count = 550**	**Est. Head Count = 10**	**Est. Head Count = 20**	**Est. Head Count = 25**	**Est. Head Count = 10**

*Teams that do not access Protected Data, such as Product & Engineering not described above, Global Business Solutions (sales), Creator & Artist Partnerships, Business Development, Communications, and Government Relations will remain at TikTok Inc. & ByteDance to ensure global business alignment.

APP-269

Independent Directors will control decision-making over National Security Functions

TikTok U.S. Ops Board

ByteDance Director

ByteDance Director

Security Committee

Security Director / Chairperson of the Board

Security Director

Security Director

Independent Security Directors approved by the CMAs will hold a majority position on the TikTok U.S. Ops Board with respect to non-National Security Functions.

National Security Function decision-making is **solely vested in the Security Directors.**

ByteDance directors (which may be from TikTok Inc. or TikTok Ltd.) add business experience and expertise and help ensure alignment on objectives with the ROW business

APP-270

TikTok U.S. Ops – Multi-Layered Operational Security and Governance

TikTok U.S. Ops Board *Directors*

| Security Director | Security Director | Security Director |

Security Committee

Security Officer & Key Management Personnel

Employees with Access to Protected Data

Trusted Technology Provider
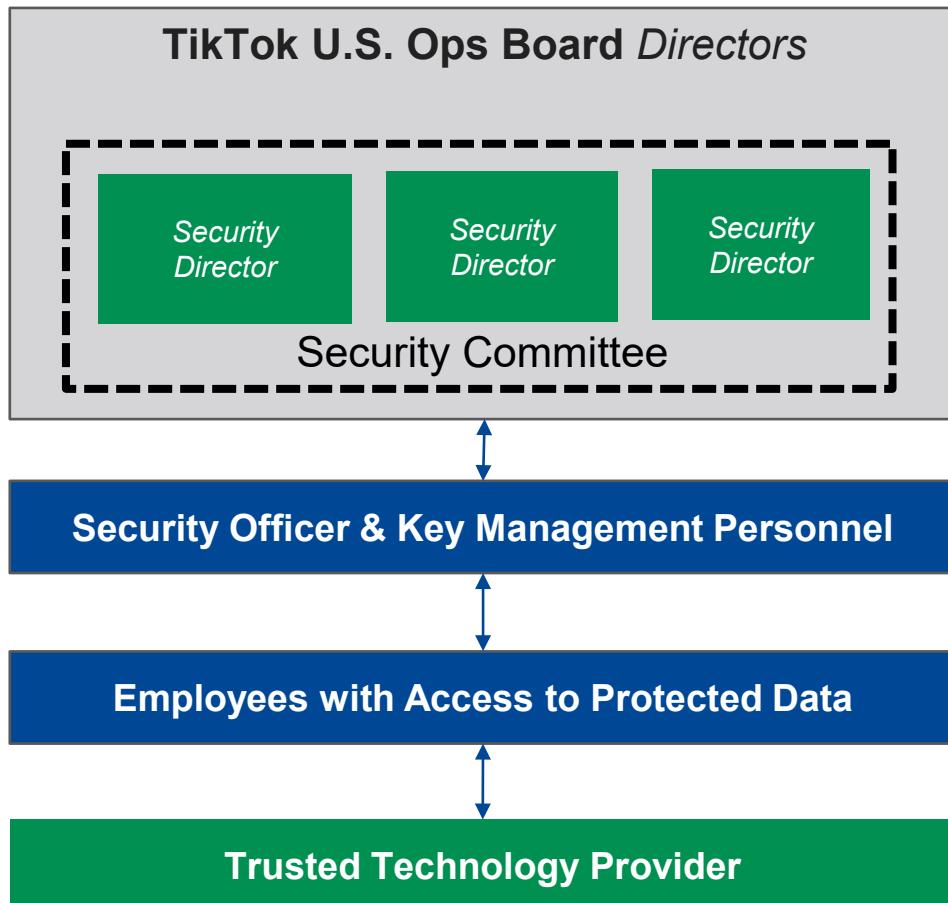
- ✓ CMA review and approval at almost every level
- ✓ Security Committee has sole authority for key national security decisions related to Privacy and Data Security, Cybersecurity, and National Security
- ✓ Citizenship and Residency Requirements for key roles and responsibilities
- ✓ Hiring Protocols for all employees
- ✓ Outsourced Protected Data storage and Software Assurance to independent and trusted third party in TTP
- ✓ No direct reporting relationship of TikTok U.S. Ops personnel to ByteDance personnel
- ✓ Access to Protected Data will be on a need-to-have basis
- ✓ TTP grants, controls, and monitors all Access to Protected Data
- ✓ TTP ultimately has the ability to suspend the U.S. TT App and TT U.S. Platform

APP-271

TikTok Inc. & TikTok U.S. Ops Alignment

TikTok Inc.

Key Functions*

- Global Business Solutions / Sales
- Creator & Artist Partnerships
- Business Development
- Marketing
- Global Security
  (Alignment to ensure the safety of users worldwide)
- Global Product & R&D
- Global Trust & Safety
- Global Operations

*Personnel who work for the TikTok United States business and maintain global alignment & interoperability.

TikTok Inc. will continue to manage non-US National Security Functions

TikTok Inc. and TikTok U.S. Ops coordinate with respect to National Security Functions between U.S. and ROW platform.

TikTok U.S. Ops

Key Functions

- Ads Integrity & Reporting
- U.S. Trust & Safety
  (U.S. policy development & enforcement)
- U.S Security
  (Securing the safety of U.S. users)
- Subset of Product & R&D
  (Ensure stable deployment of TikTok App in the U.S.)
- U.S. User & Product Operations
- Insights & Analytics
- HR, Legal, and other support

Trusted Technology Provider

APP-272

11

Robust Independent Monitoring for Compliance

CFIUS has multiple monitoring & oversight roles available to ensure TikTok U.S. Ops, TikTok Inc., and ByteDance's ("Transaction Parties") continued compliance with NSA obligations – above and beyond governance structure.

One-Time Cybersecurity Audit	• TikTok U.S. Ops will submit to a one-time cybersecurity audit of the TikTok U.S. Platform by a U.S.-based independent third party to ensure the Transaction Parties compliance with their NSA obligations.
Third-Party Auditor	• The CFIUS Monitoring Agencies may request an annual audit by a U.S.-based third-party independent auditor to assess the overall compliance with the NSA by the Transaction Parties.
Third-Party Monitor	• TikTok U.S. Ops will engage an independent third-party, approved by and reporting to the CFIUS Monitoring Agencies, to monitor compliance with the NSA.
CFIUS Monitoring Agencies	• The CFIUS Monitoring Agencies may conduct site visits, in their sole discretion, at any of the Transaction Parties U.S. facilities for on-site reviews and audits. • The CFIUS Monitoring Agencies have approval authority over NSA protocols and processes.

APP-273

Protections Against Unauthorized Access

The Proposed Structure is tailored to secure National Security Functions without restricting interoperability of the global business.

Concern	Oversight	
	Solution	**Owner**
Access to Protected Data	No Unauthorized Access to Protected Data	Trusted Technology Provider
Hiring an Insider Threat	Independent hiring for positions with access to Protected Data	Independent Governance
Software Backdoor	Independent software assurance process	Trusted Technology Provider
Content	Multiple layers of oversight against national security bias	Security assurance of software by TTP; Security Directors provide oversight, supported by Content Advisory Council

APP-274

Benefits of Proposed Governance Structure

1	Clear segregation of National Security Functions and clear mission for TikTok U.S. Ops
2	Preservation of interoperability across global and U.S. platforms • Maintain globally integrated operations and management for aspects of business that do not involve National Security Functions
3	Preservation of consistent global user experience
4	Better enable continued attraction of creators, advertisers, and talent within the organization and alignment on key business objectives
5	We believe that this approach will address Chinese regulatory concerns

APP-275

The parties look forward to continuing to engage with CFIUS to complete an NSA that fully resolves any U.S. national security concerns.

APP-276

Exhibit D

Redacted Version

ByteDance

TikTok

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States
October 13, 2021

ByteDance Participants (telephonic)
- **Erich Andersen** – General Counsel and Head of Corporate Affairs
- **Vanessa Pappas** – TikTok Chief Operating Officer
- **Will Farrell** – TikTok Head of Global Cyber and Data Defense
- **Sandie Hawkins** – GM of North America, Global Business Solutions
- **Matt Penarczyk** – TikTok Head of Legal, Americas
- **Sarah Aleem** – TikTok Senior Legal Counsel, North America

Oracle Participants (telephonic)
- **Edward Screven** – Chief Corporate Architect
- **Craig Stephen** – Senior Vice President, Research and Development
- **Scott Gaetjen** – Vice President, Cloud Chief Architect
- **Brian Higgins** – Senior Vice President, Legal

Counsel
- **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **Monty Roberson**(Covington) on behalf of ByteDance
- **Giovanna Cinelli** and **Christian Kozlowski** from Morgan Lewis on behalf of Oracle

APP-278

Topics for Today's Discussion

1	Data Governance Objectives & Development Process
2	Review of Proposed Model
3	Protected Data, Exceptions and Use Cases
4	Business Concerns
5	Conclusions and Q&A

APP-279

Key Data Governance Objectives

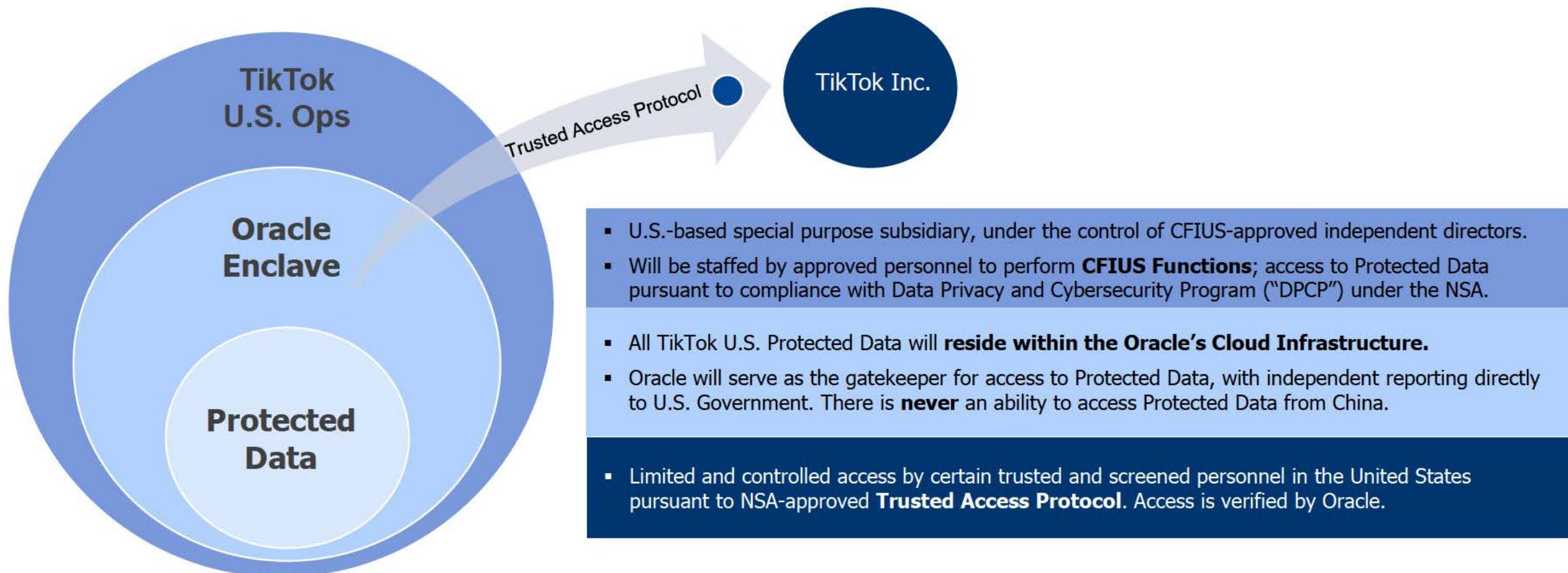Safeguard Protected Data in a manner that conforms with U.S. government national security objectives.

Maintain a global, interoperable short-form video platform business that ensures continued consistency between U.S. and non-U.S. user experiences.

Implement an operationally feasible agreement that has robust, sustainable compliance and oversight functions as the business evolves.

APP-280

Overview of Use Cases

Category	👤 Users	Creators	📢 Advertisers
TikTok Use Cases	• Watch global content • Engage with other global users (e.g., likes, comments, direct messages, share videos)	• Publish videos, go viral, and gain a following of global online users • Monetize through on-platform opportunities (e.g., Creator Fund) • Connect with advertisers for further on- and off-platform monetization opportunities	• Amplify their brands globally • Reach a specific audience segment to sell merchandise
	Participate in a global platform that is safe and reliable		
Expectations for the TikTok Experience	• Address account inquiries (e.g., password reset) through our User Support teams	Work with TikTok Content teams to: • Improve their on-platform performance using core metrics (e.g., finish rates) • Take part in programs to amplify and monetize their content	Collaborate with our Sales teams to: • Use core business metrics (e.g., clicks, views) to understand their audience • Measure ROI to optimize campaign performance

APP-281

Conceptual View of Protected Data Model

All Protected Data is controlled and isolated within at least two circles of trust: Oracle & TikTok U.S. Ops.
Oracle, as the Trusted Technology Provider, stores and controls all access to Protected Data on the TikTok U.S. Platform to ensure that data is only accessed as allowed by the NSA, including no access by <u>unauthorized persons</u> or <u>from China</u>.

TikTok U.S. Ops

Trusted Access Protocol

TikTok Inc.

Oracle Enclave

Protected Data

- U.S.-based special purpose subsidiary, under the control of CFIUS-approved independent directors.
- Will be staffed by approved personnel to perform **CFIUS Functions**; access to Protected Data pursuant to compliance with Data Privacy and Cybersecurity Program ("DPCP") under the NSA.

- All TikTok U.S. Protected Data will **reside within the Oracle's Cloud Infrastructure.**
- Oracle will serve as the gatekeeper for access to Protected Data, with independent reporting directly to U.S. Government. There is **never** an ability to access Protected Data from China.

- Limited and controlled access by certain trusted and screened personnel in the United States pursuant to NSA-approved **Trusted Access Protocol**. Access is verified by Oracle.

5

Architecture View of Data Protection System

APP-283

What is Protected Data?

**There is substantive alignment on the NSA data definitions.
All data of TikTok U.S. Users falls within one of the following 3 categories:**

Protected Data is all data collected or derived from a TikTok U.S. User that is not: • **Excepted Data,** or • **Public Data**	**Excepted Data** includes: • Engineering and Business Related Metric data (i.e. dashboard-type); and • Interoperability data (for convenience, we refer to these as "flags")	• **Public Data** is data that is generally accessible to public users of the TikTok U.S. platform

APP-284

Protected Data: Who is a "U.S. User"?

There are two ways a user becomes a TikTok U.S. User:

| 1. Individuals signing into the TikTok App – categorized based on location	2. If <u>not</u> captured in #1, users who want to be categorized as TikTok U.S. Users may opt-in
Users located in the United States based on (in order of priority): • Country code of device subscriber identity module (SIM) card; • IP address; • Mobile country code associated with mobile subscription of the device; or • OS/System Region	*E.g.*, Expat U.S. citizens requesting reclassification pursuant to CMA-approved protocol • Will include option to select at new user registration • Push notification to existing users to alert them to new feature • Feature within all versions for users to be reclassified as TikTok U.S. Users

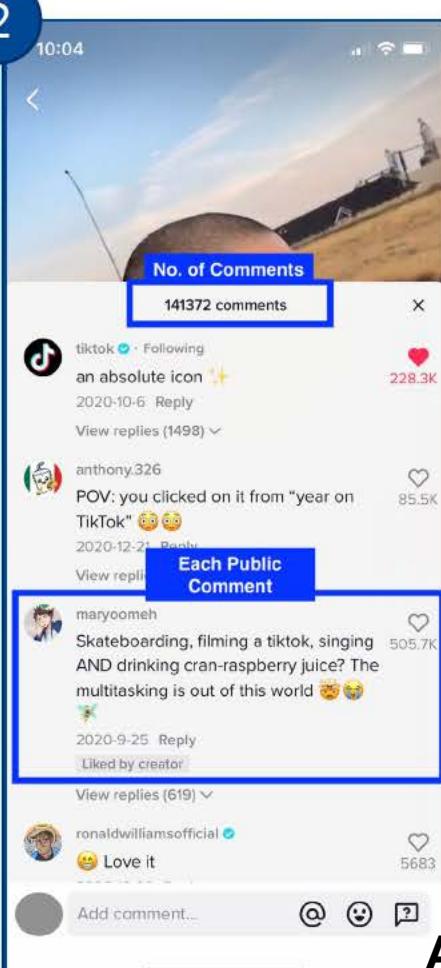**APP-285**

Video Demonstration – Public Data

APP-286

9

Public Data: In-App View

APP-287
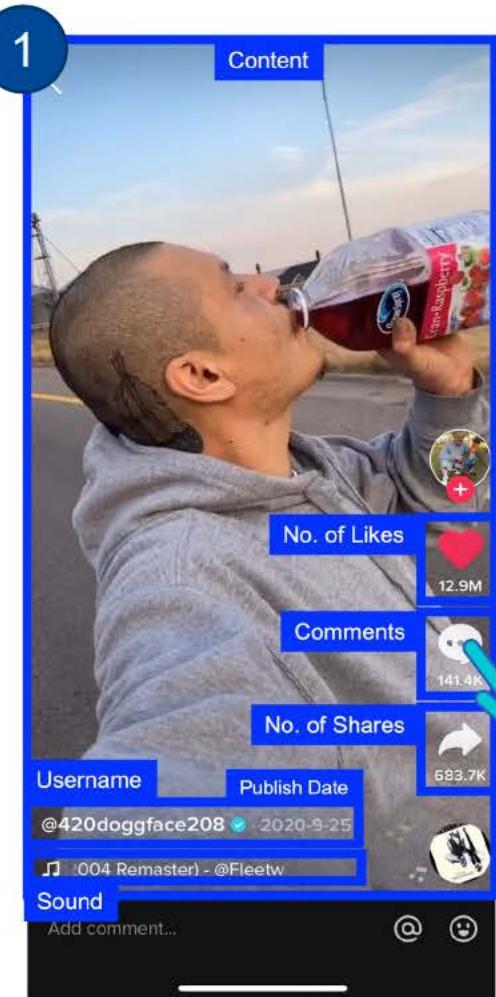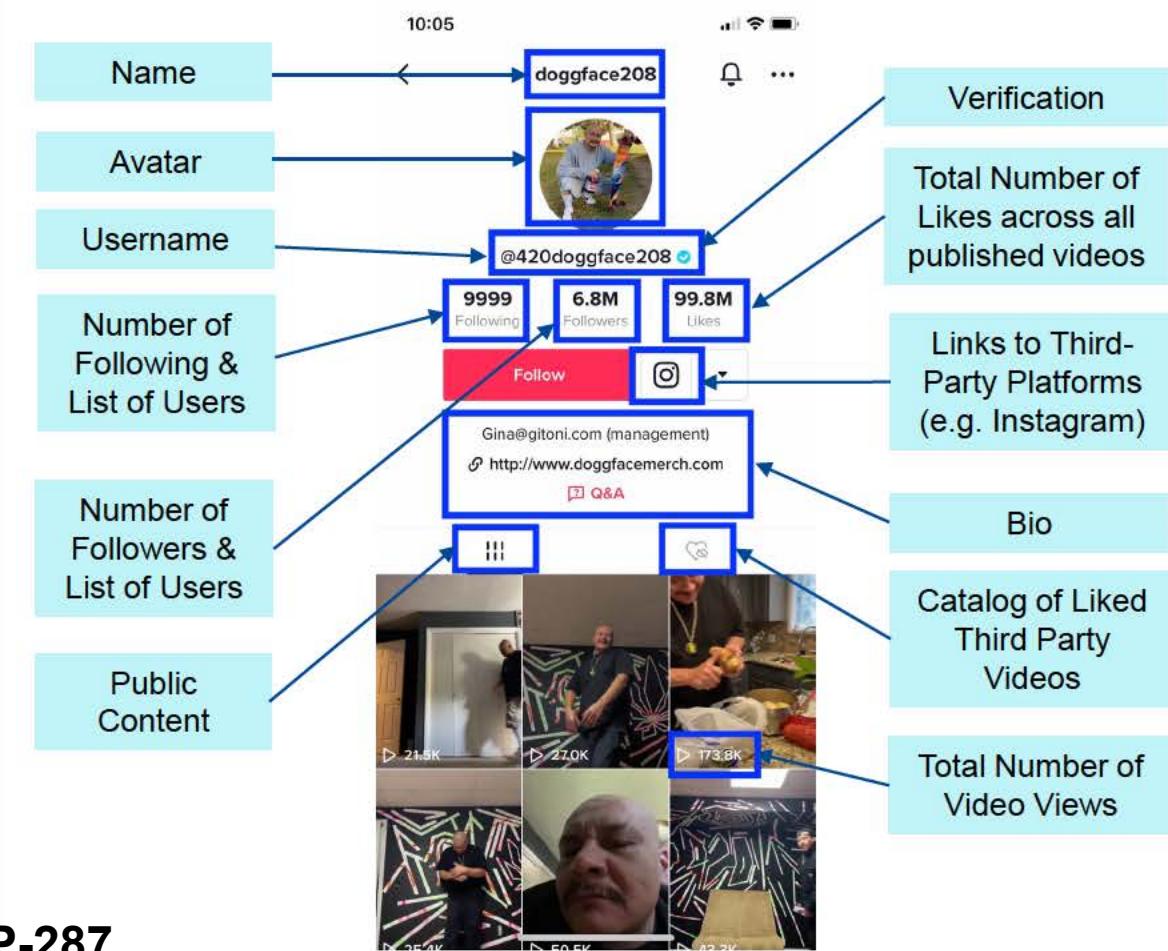
Public Data: Web View

Web View

Username & Publish Date

Number of Likes & Comments

Public Comments

Public URLs
a. Truncated URL:
https://vm.tiktok.com/ZM81NUkx8/

b. Full URL:
https://www.tiktok.com/@420doggface208/video/6876424179084709126?lang=en&is_copy_url=0&is_from_webapp=v1&sender_device=pc&sender_web_id=6893557692481422853

Video ID

Language

APP-288

Excepted Data - Interoperability

Public data alone is insufficient to maintain TikTok as a global platform.

- Video creators can choose settings on videos not public to other users.
  - For instance, users can choose to make videos private.
- When public videos are determined by TikTok systems to be both safe and popular, they are sometimes distributed globally (e.g., U.S. videos shared to the U.K. or Australia).
- To support the global distribution, it is important that certain flags associated with those videos, such as public/private settings, travel with the videos on global systems so as to respect user choices.

TikTok also wants to continue to support users who want to send private messages to users in other countries.

APP-289

Use Case 1: User Wants to Publish <u>Public</u> Video

1
- User creates a video they want to upload and make public
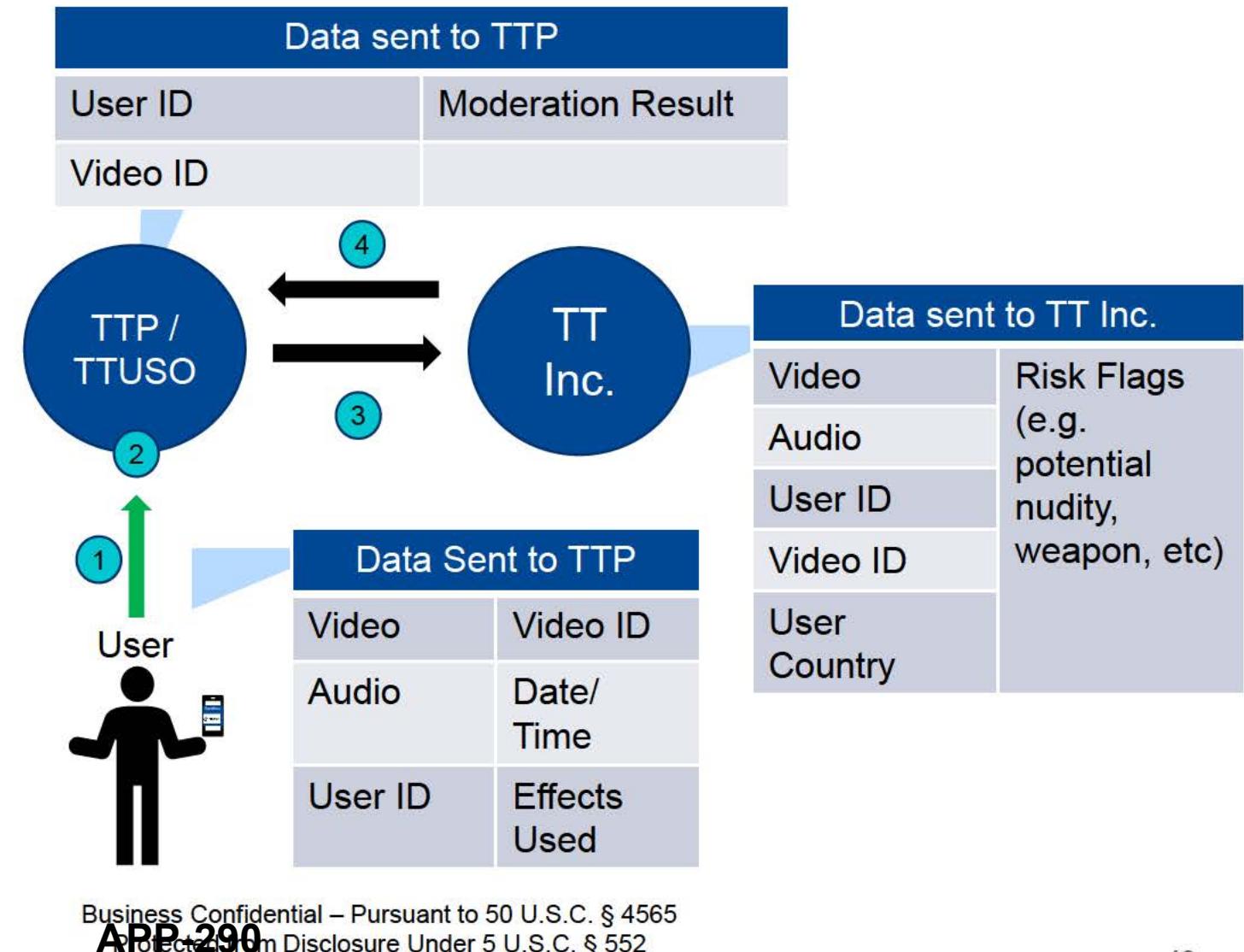- Video is uploaded to TTP cloud infrastructure

2
- Video and account information is processed by TTUSO / TTP to identify any safety risks

3
- If Risk is Flagged:
  - Video passes through data exchange system and is stripped of User Data except for interoperability flags, UID, and VID and sent to TT Inc. for Global Moderation
  - Public Video may be "Human Reviewed" based on risk flags from analysis in TTP

4
- Moderation Decision is Recorded and Returned to TTP
  - Safe / Video Takedown / Account Ban

Data sent to TTP

User ID	Moderation Result
Video ID	

Data sent to TT Inc.

Video	Risk Flags (e.g. potential nudity, weapon, etc)
Audio	
User ID	
Video ID	
User Country	

Data Sent to TTP

Video	Video ID
Audio	Date/Time
User ID	Effects Used

TTP / TTUSO
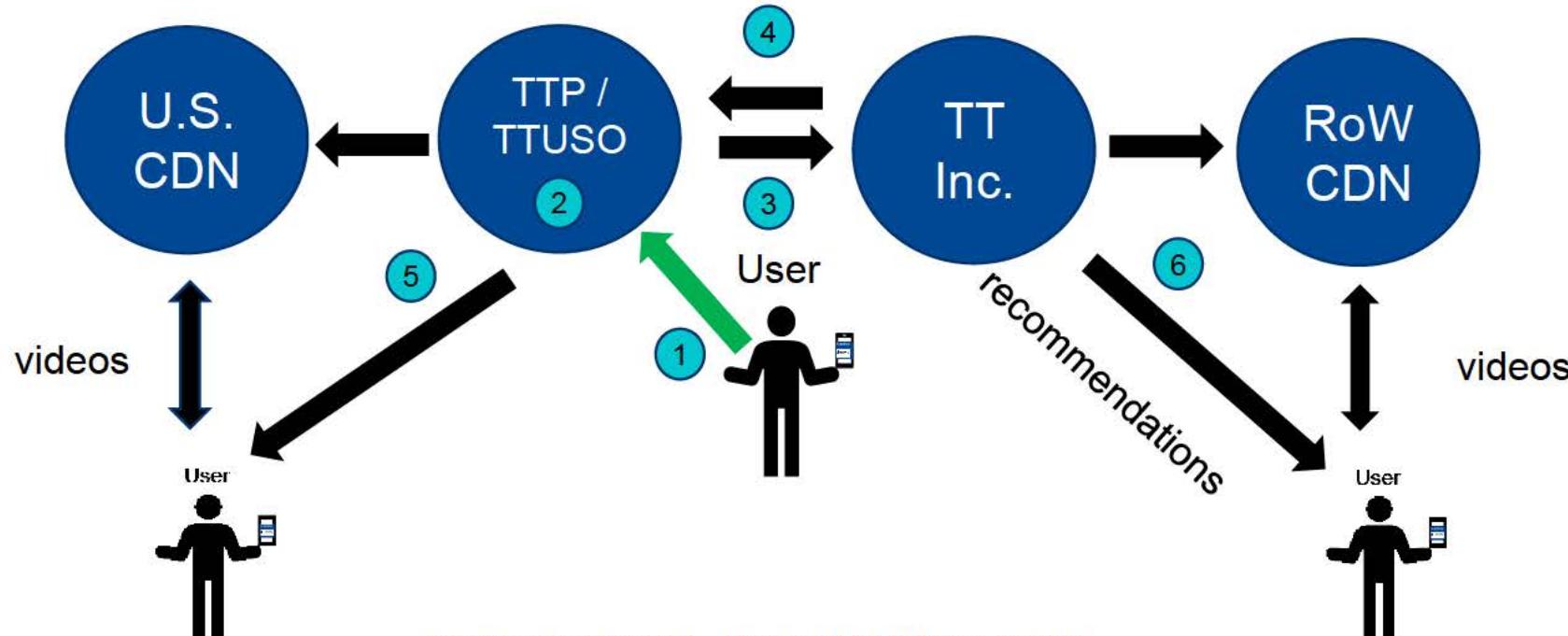
TT Inc.

User

APP-290

Use Case 1: User Wants to Publish Public Video

5 • Video is included in recommendations and shared with U.S. Users via U.S. CDN

6 • If video begins to get popular and is potentially relevant / popular to other markets:
  - TT Inc. will begin recommending it for users in relevant markets
  - TT Inc. will distribute video through RoW CDNs

APP-291

14

Use Case 2: User Decides to Change Status of Video to Private

7 User changes status of video or account to private

8 Message is exchanged with TT Inc. and CDNs to remove content to protect user's privacy

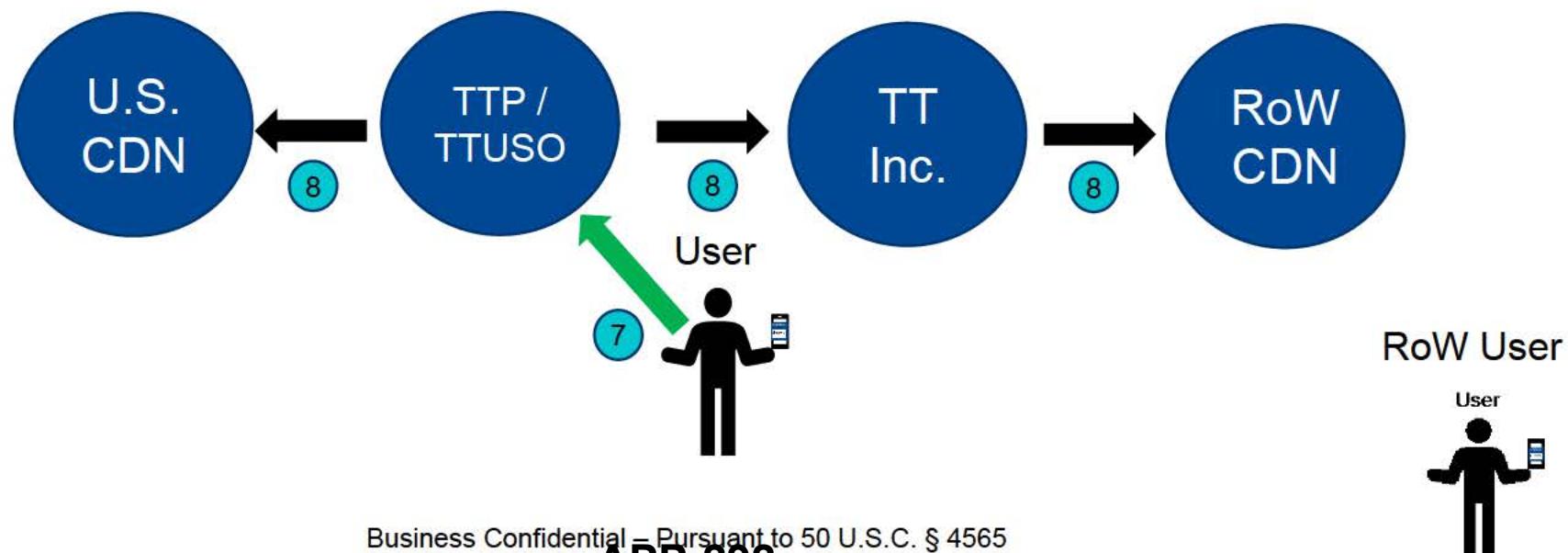| Data sent to TT Inc. |
|---|
| User ID |
| User Status (Flag) |
| Video ID |
| Video Status (Flag) |

U.S. CDN ← TTP / TTUSO → TT Inc. → RoW CDN

8   8   8

7 User

RoW User

User

APP-292

Excepted Data – Engineering and Business Metrics

The global leadership team follows high-level metrics, such as daily active users in the U.S., to assess overall performance.

The global engineering development teams access certain metrics derived from U.S. user data (presented in dashboard form) to improve products and make technology-related decisions: Examples include:
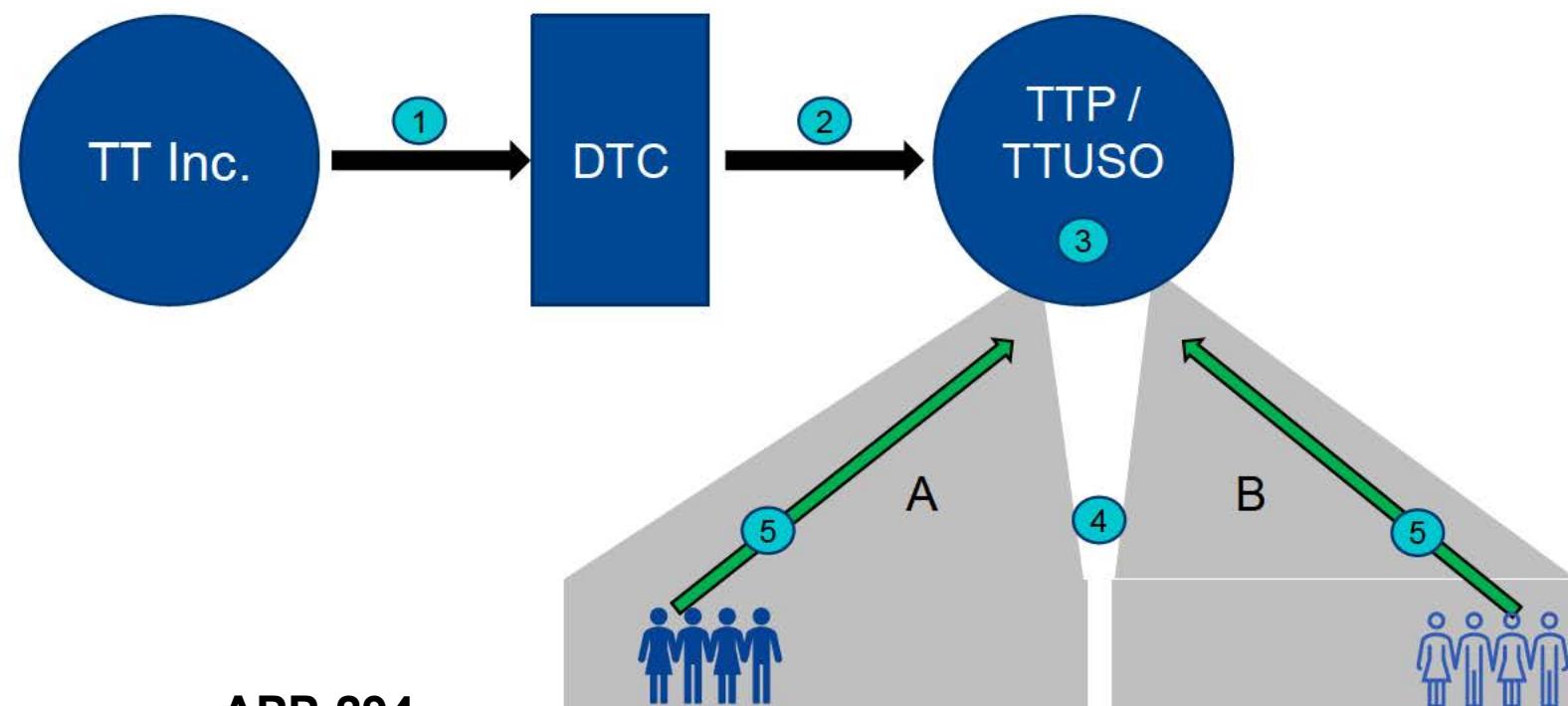- Feature usage in order to understand what features actually solve a user's problems to better optimize the product
- Video view trends and session length to decide on future capital expenditures on IT infrastructure (e.g. servers)

The global advertising sales and creator engagement teams also use metrics data, for example, to assess and explain the outcome of advertising campaigns to customers.

APP-293

Use Case 1: Engineering Data: A/B Feature Testing

1 • The Engineering team wants to see if a new feature will resonate in the U.S. users
  - The code is developed and delivered to the DTC

2 • TTP analyzes the code to determine if safe and appropriate for deployment

3 • TTUSO / TTP generate two randomized samples of users (control group and test group)

4 • TTUSO / TTP deploys the update to the test group

5 • TTP collects engagement metrics from the users in the test group and control group

TT Inc. → ① → DTC → ② → TTP / TTUSO ③

A ⑤ ④ B ⑤

APP-294

17

Use Case 1: Engineering Data: A/B Feature Testing

6 • TTUSO / TTP generates metrics reporting, ensuring no individual user records are included

7 • Reporting is returned to TT Inc. for the Engineering team to determine how the new update was received compared to the control group

Sample Engineering and Business Metrics

• Total/Average/Percentage of users that are exposed to a product feature by experiment group, time period, account property and status, action placement and history, device attributes, network environment and video attributes

• Total/Average/Percentage of users that interact with product by experiment group, time period, account property and status, action placement and history, device attributes, network environment and video attributes

7

TT Inc. → **1** → **DTC** → **2** → **TTP/ TTUSO** **6** **3**

A **5** **4** **B** **5**

APP-295

18

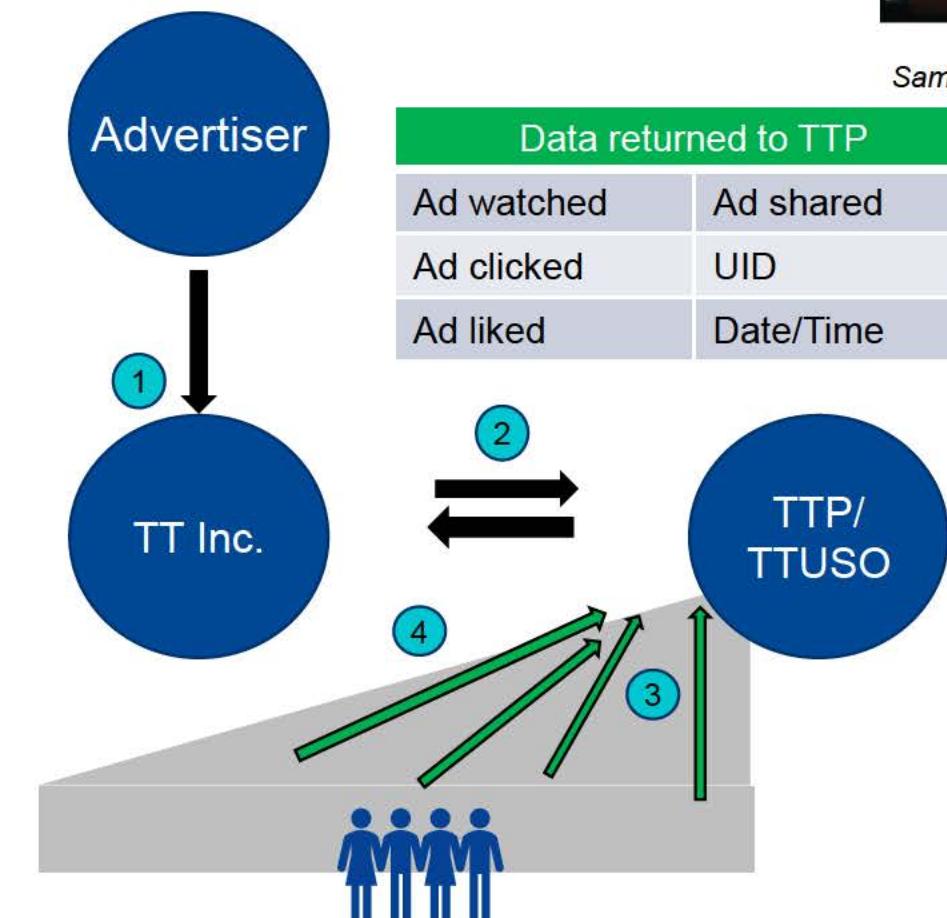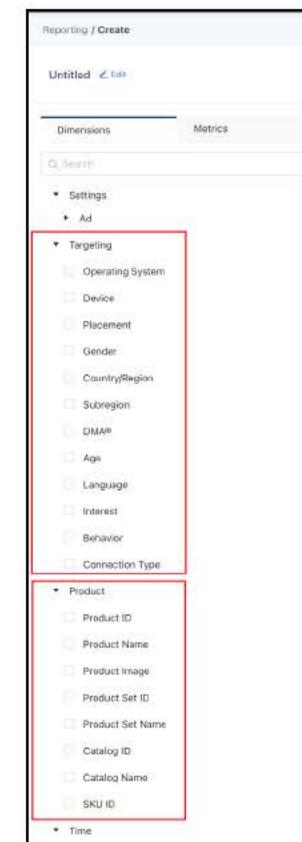# Use Case 2: Advertising: Create Global Ad Campaign

APP-296

Use Case 2: Advertising: Create Global Ad Campaign

Sample Ad

1 • Advertiser sends Ad and desired audience segment information to TT Inc.

2 • If there is U.S. audience, TT Inc. sends same Ad and audience segment to TTP/TTUSO

3 • TTUSO tasks Ad system within TTP to the appropriate audience segment

4 • Subset of users will see the Ad and may click on the Ad

Reporting / **Create**

Untitled ✎ Edit

Dimensions | Metrics

Q Search

▼ Settings
  ▸ Ad
▼ Targeting
  ☐ Operating System
  ☐ Device
  ☐ Placement
  ☐ Gender
  ☐ Country/Region
  ☐ Subregion
  ☐ DMA®
  ☐ Age
  ☐ Language
  ☐ Interest
  ☐ Behavior
  ☐ Connection Type
▼ Product
  ☐ Product ID
  ☐ Product Name
  ☐ Product Image
  ☐ Product Set ID
  ☐ Product Set Name
  ☐ Catalog ID
  ☐ Catalog Name
  ☐ SKU ID
▼ Time

Advertiser

1

TT Inc.

2

TTP/ TTUSO

3

4

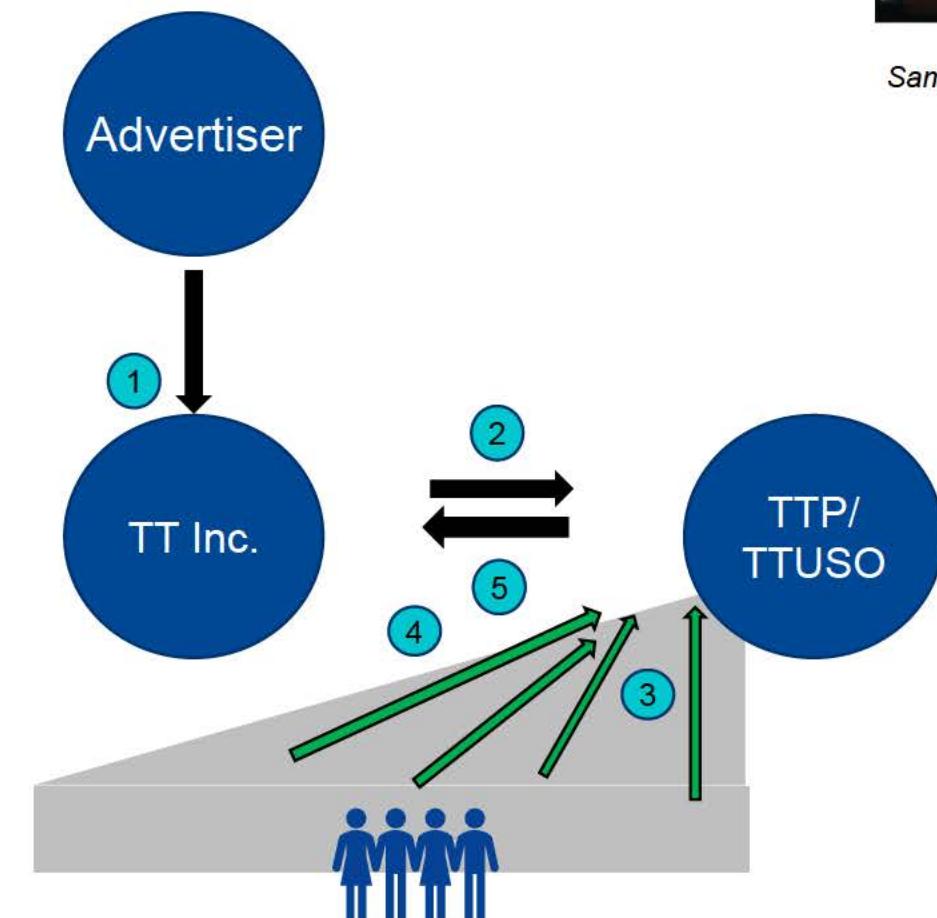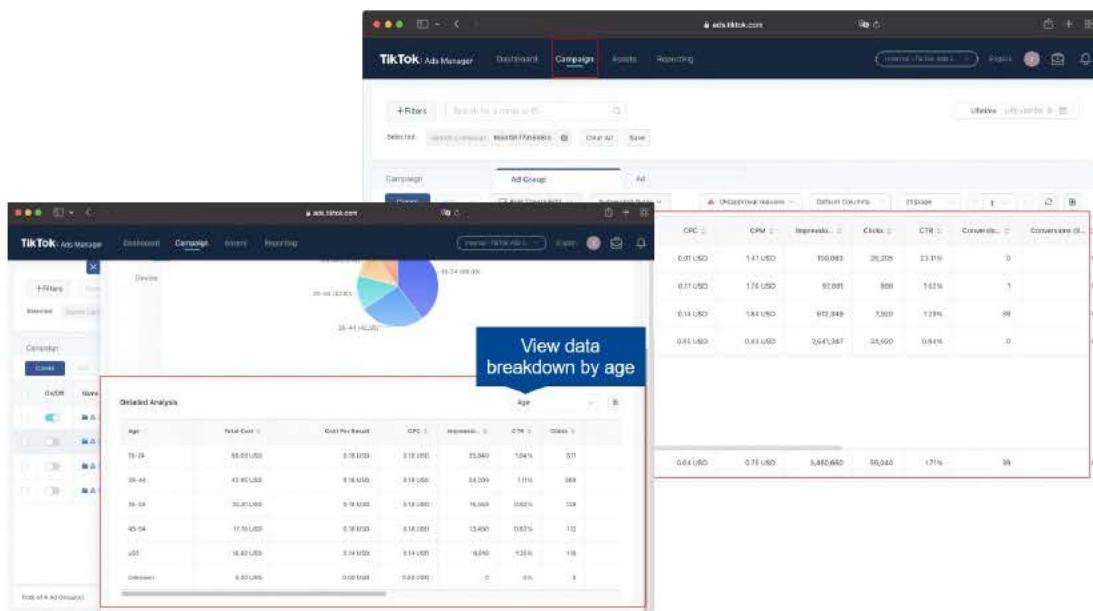| Data returned to TTP	
Ad watched	Ad shared
Ad clicked	UID
Ad liked	Date/Time

APP-297

Use Case 2: Advertising: Create Global Ad Campaign

Sample Ad

5 • TTP/TTUSO returns Metrics / Reporting to TT Inc. (no individual records, only totals and %)

Advertiser

TT Inc.

TTP/ TTUSO

1

2

5

4

3

View data breakdown by age

APP-298

Example of TikTok Ads Manager Dashboard View:

APP-299

Example of TikTok Ads Manager Dashboard View:

View data breakdown by age

Detailed Analysis

Age

Age	Total Cost	Cost Per Result	CPC	Impressio...	CTR	Clicks
18-24	66.09 USD	0.18 USD	0.18 USD	35,840	1.04%	371
35-44	42.95 USD	0.16 USD	0.16 USD	24,209	1.11%	269
25-34	22.81 USD	0.18 USD	0.18 USD	15,558	0.82%	128
45-54	17.76 USD	0.16 USD	0.16 USD	13,456	0.83%	112
≥55	16.92 USD	0.14 USD	0.14 USD	8,818	1.35%	119
Unknown	0.00 USD	0.00 USD	0.00 USD	0	0%	0

Total of 4 Ad Group(s)

APP-300

Use Case 2: Advertising: Create Global Ad Campaign

6 Metrics / Reporting Combine

TT Inc. combines Metrics / Reporting from US with RoW and provides to Advertiser (no individual records, only totals and %)

Advertiser

TT Inc.

TTP/ TTUSO

APP-301
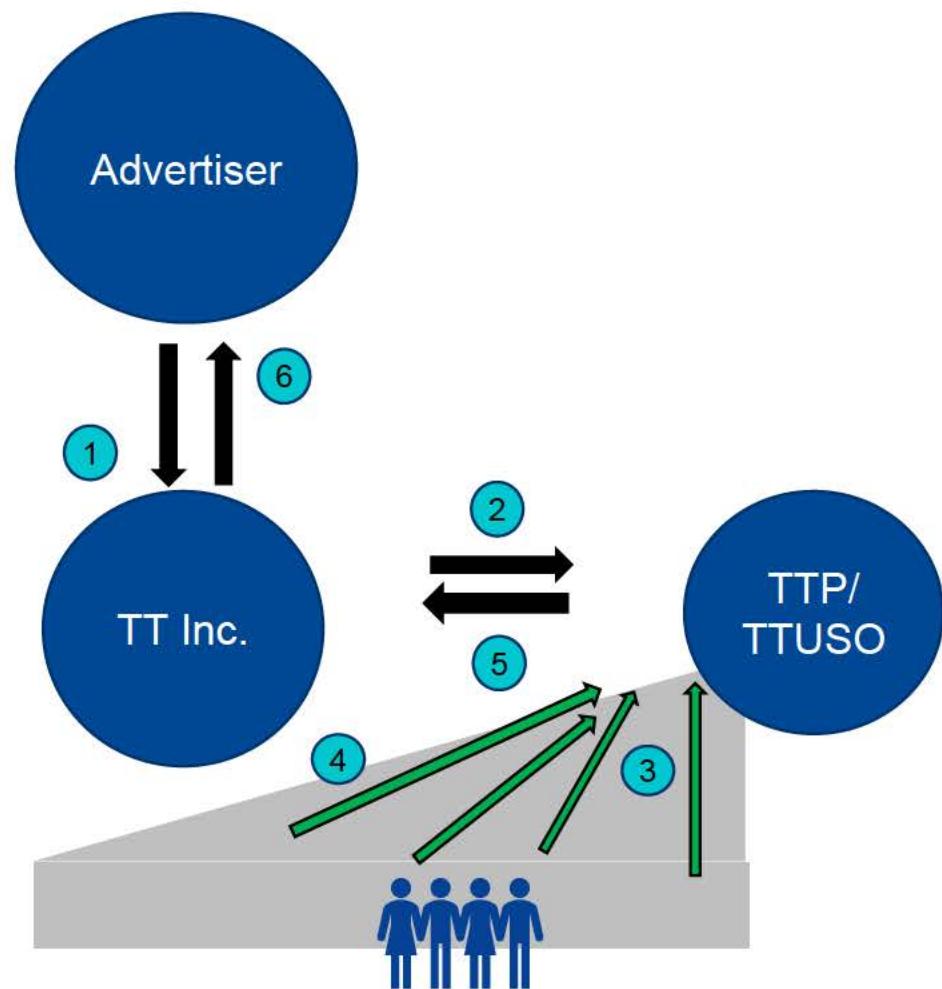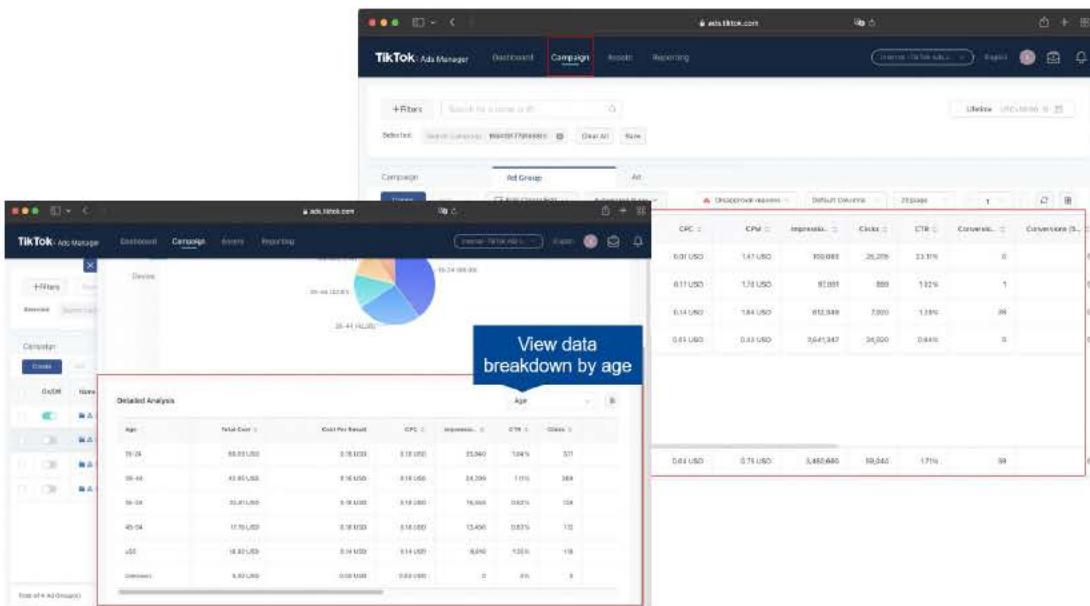
Data Removal

Proactively identifying environments for Protected Data:

- In U.S., Singapore, and China data centers
- Across 18 different database and file storage types
- With plans for e-mail and other internal systems

Developing irreversible deletion methods for all database and file storage types:

NIST 800-88 "NIST Clear"

input

Individual record deletion

considers

- **Deletion mechanics**
- **Established grace periods**
- **Backup requirements**
- **Forensic validation of deletion**

Reviewed definitions and proper sanitization methods

Developed deletion method for each database type

Applies to all U.S. data outside of Oracle environment
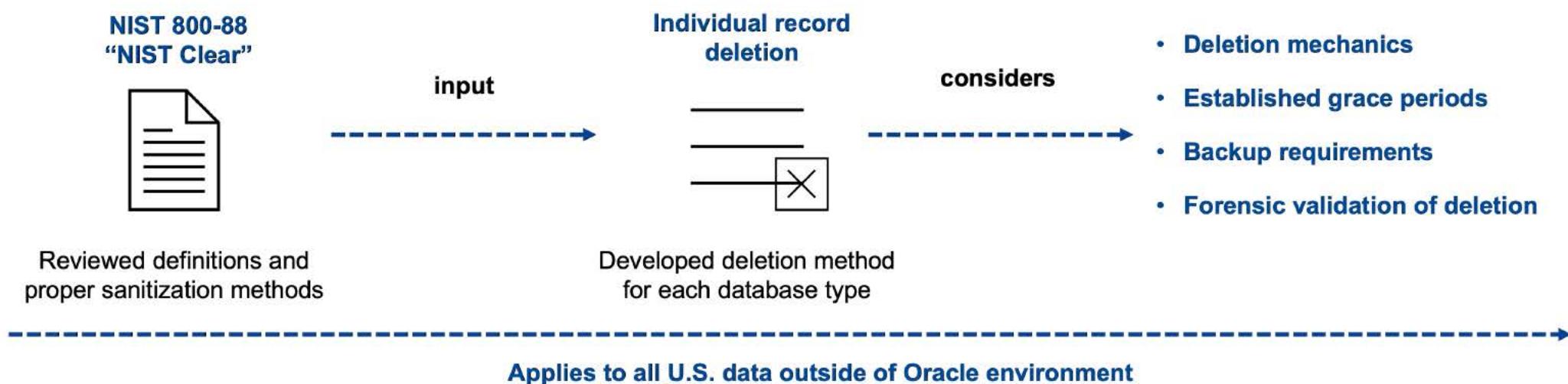
TikTok Inc. Access to Protected Data via the Trusted Access Protocol

*Trusted Personnel will be provided access to Protected Data on a restricted and monitored basis for
(1) **legal and compliance** matters; and (2) Certain other **emergency situations involving the health and safety** of TikTok U.S. Users.*

Protected Data access for the purpose of Trust & Safety will largely be accessed and used by personnel within TikTok U.S. Ops to ensure the safety and security of U.S. Users.

In exceptional cases, vetted Trusted Personnel in TikTok Inc. may need to access minimum necessary Protected Data via a Trusted Access Protocol to:
- Investigate and respond to law enforcement requests addressing **imminent harm** (e.g. investigating potential coordination of bomb threats via DMs on 9/11 in NYC).
- Investigate and take down harmful content (e.g. graphic suicide proliferating in the U.S. and globally)
- Litigation & Regulatory responses

TikTok Inc. will develop the Trusted Access Protocol with the Trusted Technology Provider and subject to prior non-objection of the CMAs.

APP-303

Business Concerns with Data Governance Approach

Challenge	Explanation
Timing of rollout and system stability	• Adding new cloud services provider generally takes a year or more • The system being installed is substantially more complex than a typical cloud deployment • TikTok and Oracle have made substantial progress toward implementing an operational system in an accelerated timeframe
Performance of Data Exchange System	• The TikTok system will require a very high number of data transformations per second to operate and meet user expectations for performance • The data exchange system that has been designed to meet US national security objectives is in the early stages of testing • Until testing is completed, we will not know whether it will perform and be stable for production use
Static Annexes	• We are concerned about the method of approving exceptions solely through static annexes in the NSA that must be updated and approved manually • Allowing for a more dynamic process would align better with the speed of development and innovation

APP-304

Conclusion

The parties look forward to continuing to engage with CFIUS on each of these topics and to complete an NSA that fully resolves any U.S. national security concerns.

APP-305

Exhibit E

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States
November 29, 2021

ByteDance Participants (telephonic)	*Oracle Participants (telephonic)*	*Counsel*
• **Erich Andersen** – General Counsel and Head of Corporate Affairs	• **Edward Screven** – Chief Corporate Architect	• **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **Monty Roberson** (Covington) on behalf of ByteDance
• **Vanessa Pappas** – TikTok Chief Operating Officer	• **Craig Stephen** – Senior Vice President, Research and Development	
• **Will Farrell** – TikTok Head of Global Cyber and Data Defense	• **Scott Gaetjen** – Vice President, Cloud Chief Architect	
• **Eric Han –** Head of U.S. Safety, TikTok	• **Brian Higgins** – Senior Vice President, Legal	• **Giovanna Cinelli** and **Christian Kozlowski** from Morgan Lewis on behalf of Oracle
• **Matt Penarczyk** – TikTok Head of Legal, Americas		
• **Sarah Aleem** – TikTok Senior Legal Counsel, North America		
• **Yufan Zhu** – Head of TikTok Engineering US		

Topics for Today's Discussion

1	An Overview of TikTok Video Discovery
2	The TikTok Recommendation Engine
3	Content Moderation
4	Video Promotion and Filtering
5	Conclusions and Q&A

In App Content Discovery
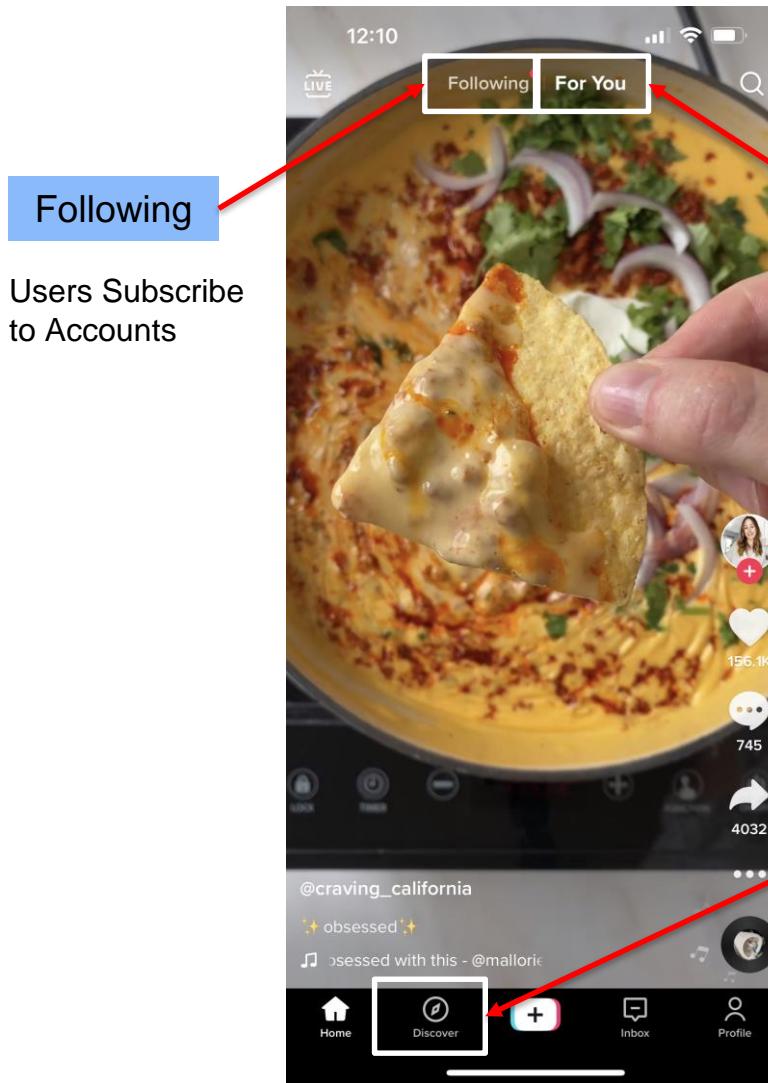
Following

Users Subscribe to Accounts

For You

The "for you" feed is central to the TikTok experience and where TikTok users spend most of their time.

Search

Discover

Programmed and Recommended Content

APP-309

3

An Overview of Steps That Determine What Users See

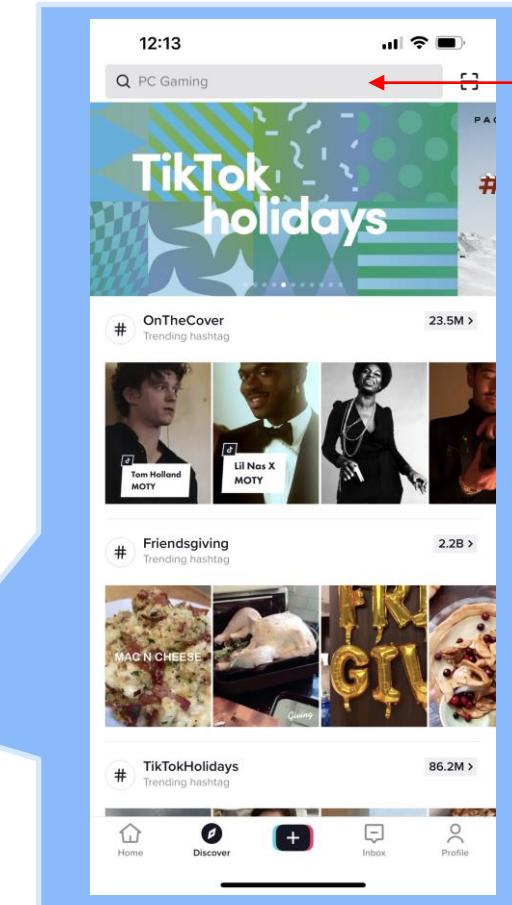| Steps	Functionality	Description
Recommendation Engine	Decide what videos are distributed to users based on content metadata and user behavior	• The **recommendation engine** is a sorting machine that decides what videos a user sees in the "for you feed" based on a statistical model developed from behavioral signals from the user and other users in the community, such as their likes, comments and watch time. Recommendation systems are common in our industry. • The **recommendation engine** does not 'understand' the content that is being recommended (e.g., whether a video is critical of a person or whether a video shows a dog or not). It does 'understand' the similarity of different videos and different people by calculating the correlations from behavioral signals of users' interactions. It's all about math - statistics and probability.
Content Moderation	Generate content selection pool for recommendation engine and moderate for compliance with community guidelines	The **content moderation system** is a hybrid system (i.e., machine and human) that is designed to implement public community guidelines and decides which content should be excluded from the pool of recommended videos based on: • Specialized computer programs that are trained to recognize categories of violating content; and • Human moderators that are trained to recognize violating content and make nuanced policy decisions. We continue to apply our **content moderation system** after videos are selected for distribution. We also have methods for users to report videos to us, for third parties to request take down where IP rights violations are infringed, and for law enforcement officials to reach out with orders to remove content.
Video Promotion and Filtering	Some videos are promoted or filtered to keep video feeds interesting, high quality and diverse	• After the recommendation engine algorithm sorts videos, we **promote** some of them to address commercial and product goals such as introducing new celebrity creators and to meet minimum commitments to advertisers. This 'heating' (promotion) process impacts less than 1% of videos. • We also applies a set of **business rules** to filter videos to support commercial and product goals such as prioritizing locally-based content, avoiding duplication, and ensuring appropriate video length.

Recommendation Engine

How this Section is Organized

1	The Basics: How does recommendation work?
2	Content Diversity: How do we ensure that users get exposed to diverse content and are not stuck in content bubbles?
3	What are the limits: What does the recommendation engine not do?

Please see Appendix for Technical Diagrams

APP-312

How "For You" Recommends Videos

Follows

Likes

Comments

Share

Captions

Hashtags

Sounds

APP-313

How "For You" Recommends Videos

APP-314

Language Preferences

Country Settings

Device Type

Recommendation Process Simplified

	Video 1	Video 2	Video 3	Video 4	Video 5	...	Video N
User 1	1	0	0	1	1	...	...
User 2	0	0	1	1	1	...	...
User 3	0	0	0	0	1	...	...
User 4	1	1	0	0	0	...	...
User 5	1	1	0	0	1	...	...
...	...	...	...	...	...	...	...
User N	...	...	...	...	...	...	...

Results – the User Experience
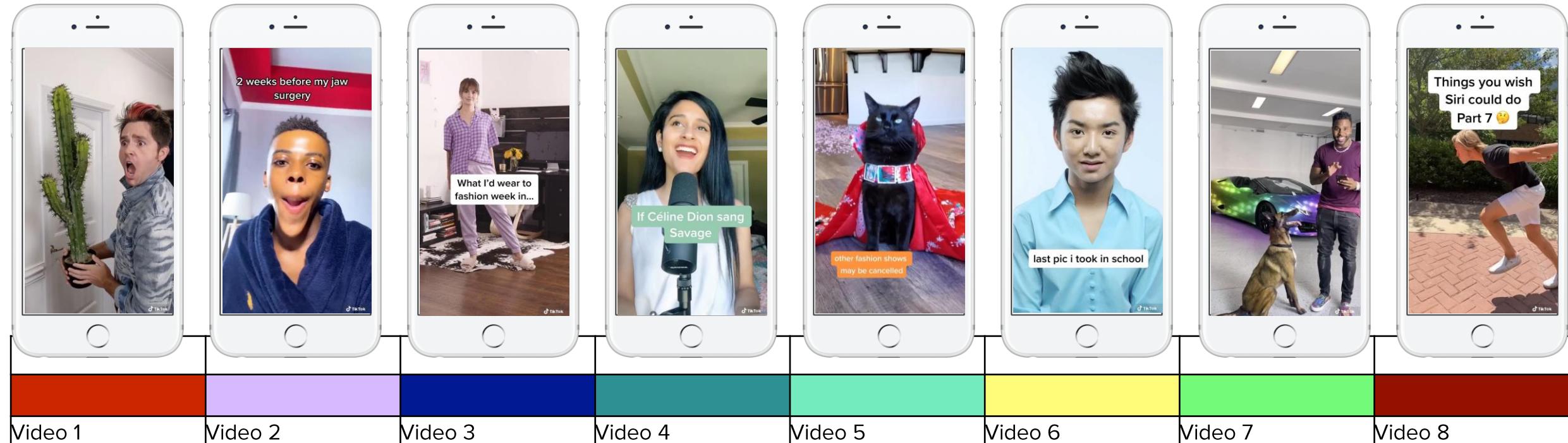
| Video 1 | Video 2 | Video 3 | Video 4 | Video 5 | Video 6 | Video 7 | Video 8 |

As a user views videos, the algorithm takes into account preferences to start grouping similar videos.

APP-316

Understanding Recommendation

As a user views videos, the algorithm takes into account preferences to start grouping similar videos.

APP-317

Understanding Recommendation

As a user views videos, the algorithm takes into account preferences to start grouping similar videos.

APP-318
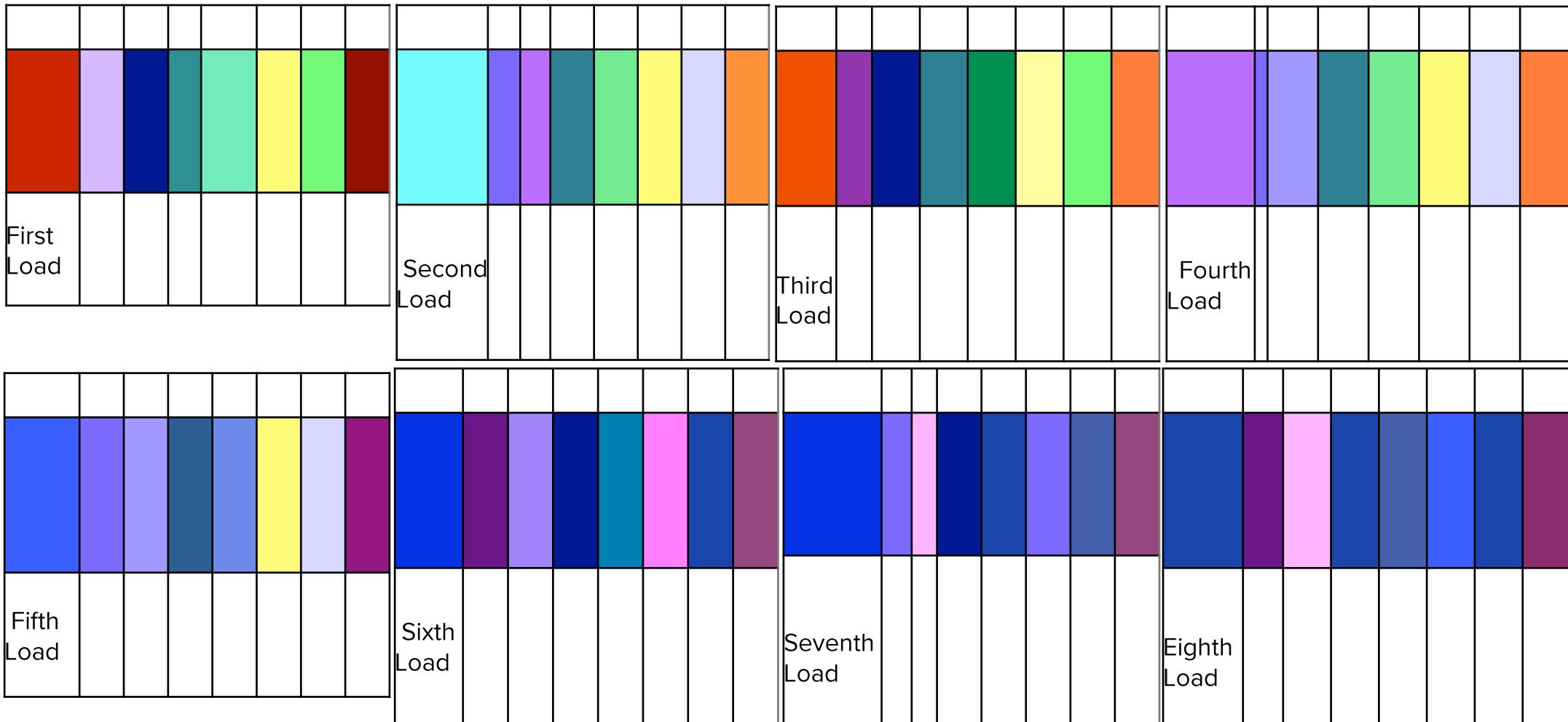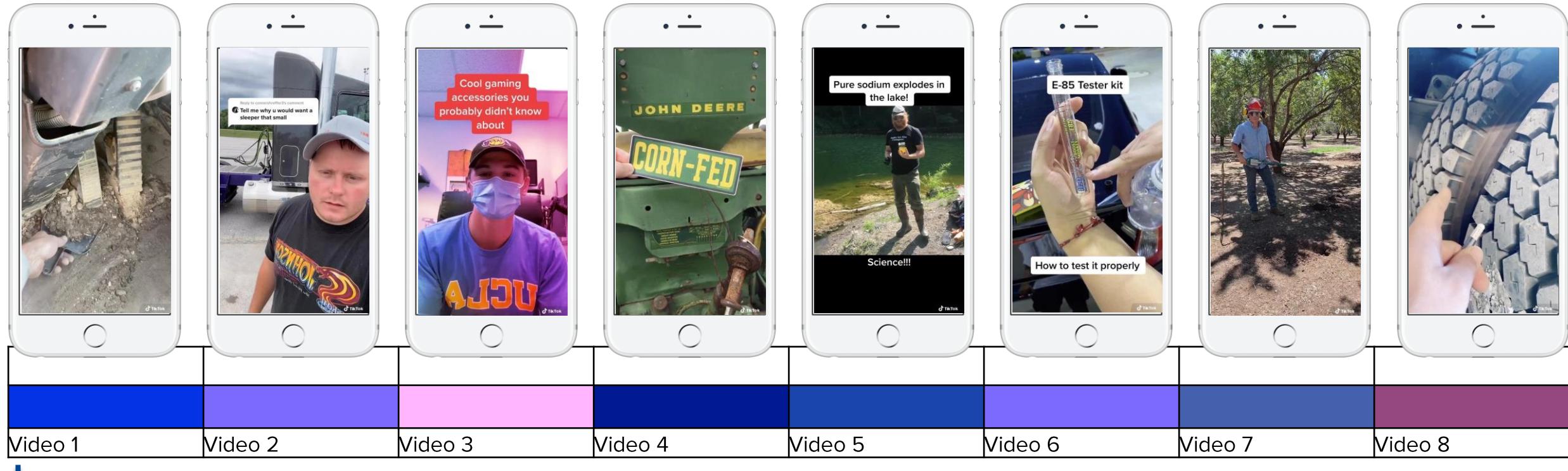
The Role of Individual Signals & Content Diversity

Each of these interaction-types ultimately influences the Recommendation Engine.

Positive Signals	Negative Signals

- ✓ Like
- ✓ Share
- ✓ Finish watching video
- ✓ Long play time
- ✓ Comment
- ✓ Follow
- ✓ Click soundtrack
- ✓ Enter creator page
- ✓ Add to favorites
- ✓ Save video

- ✗ Report
- ✗ Click 'Not Interested'
- ✗ Skip

Content diversity and user interests are critical to the recommendation system.

1. **Introduce randomization**: Randomization helps to avoid filter bubbles, content addiction, or feed polarization while enabling randomization and diversification. The algorithm down-ranks videos that are too similar to previously displayed videos and does not allow content from the same creator to continuously show on the same feed. Lastly, the algorithm will also display random videos to explore the user's interest and recommend accordingly.

2. **Prioritize recent engagement**: The algorithm assigns higher weights to more recent engagements on the platform. A user can explore new content categories more aligned to their recent engagements which evolves and diversifies the content they see.

3. **Content recycling:** Recommendation is a process of exploring and adjusting to the user's interest. If a user does not express interest in a video, it will likely not reappear. However, the content may appear as random videos in the feed, which diversifies the feed and explores potential new interest areas.

What Recommendation Engine Does <u>NOT</u> Do

X	It does **NOT** look to promote or suppress a particular political agenda, views, or content
X	It does **NOT** use signals to infer someone's race, ethnicity, sexual orientation, or political affiliation or beliefs.
X	It does **NOT** "have an agenda."

Instead, the recommendation engine is a complex set of formulas that looks to provide individually tailored content for each user.

APP-320

Content Moderation

APP-321

How this Section is Organized

Content Moderation is a continuous process managed by thousands of people and a suite of sophisticated technology that is being continually updated.

1	Community Guidelines: TikTok public policies that describe what is and what is not allowed on the platform
2	The Advisory Counsel
3	Moderation Technology: Special purpose models that check for and remove unauthorized content an help respond to user and law enforcement requests

TikTok's Community Guidelines

By protecting the safety of our users, we create a positive environment for our community.

☀	Ensure that TikTok is a place for inclusive, joyful, and authentic content -- a place where users can safely discover, create, and connect.
🛡	Our Trust & Safety teams provide the policies, operations, strategies, and technologies to ensure that the TikTok community is protected against any and all threats in the U.S. and worldwide.
🤝	We consider local laws, as well as cultural and social norms, and engage multiple external stakeholders in developing our content moderation policies.
📋	Community Guidelines are public and available here: www.tiktok.com/community-guidelines

APP-323

Community Guidelines Principles

*The TikTok **Community Guidelines** are a publicly available code of conduct to ensure user safety and a friendly digital environment. A violation of the guidelines may result in the account and/or content being removed.*

❌ Dangerous individuals and organizations	❌ Suicide, self-harm, and dangerous acts	❌ Hate Speech	❌ Violent and graphic content	❌ Illegal activities and regulated goods
❌ Adult nudity and sexual activities	❌ Harassment and bullying	❌ Content harmful to minors	❌ Integrity and authenticity	❌ Threats to platform security

Content Advisory Council

*On March 18, 2020, TikTok announced the inaugural members of the **TikTok Content Advisory Council** to advise the business on a variety of topics, including child safety, hate speech, misinformation, and bullying, with members hailing from the technology, policy, and heath and wellness industries.*

Content Advisory Council Member	Affiliation
Dawn Nunziato, Chair	George Washington University School of Law
Hany Farid	University of California - Berkeley School of Information
David Polgar	All Tech is Human
Vicki Harrison	Stanford Center for Youth Mental Health and Wellbeing
Marry Anne Franks	University of Miami Law
Rob Atkinson	Information Technology & Innovation Foundation
Dan Schnur	University of Southern California Annenberg Center on Communication Leadership & Policy
Dorothy Espelage	University of North Carolina School of Education
Mutale Nkonde	Berkman Klein Center for Internet & Society at Harvard University

Content Moderation Overview

*TikTok has combined content moderation technology with a robust human moderation team and several layers of tools and processes to recommend **safe** content to users.*

1 AI Safety Models	**2** User Reporting	**3** Virality Check
• Intelligent safety models **are** built on text, video, image and behavioral signals to identify content that may violate the Community Guidelines. • AI Safety models continuously monitor content. • May result in automatic takedowns without human moderation.	• Any video can be reported and flagged for review. • Users can report through in app reporting mechanism • Third parties can report (e.g., copyright, underage user) through webforms.	• Certain viewership thresholds of virality lead to mandatory human review. • Serves as an additional check on widely distributed.

Human Moderation teams review content after receiving signals from above.
Human review may include multiple rounds of review.

APP-326

Human Moderation Interface

APP-327

Incident Management

Bad actors are constantly trying to circumvent our systems. Our incident management teams proactively monitor the content on platform to hunt for these culprits, and to adapt, learn, and evolve our systems to be one step ahead of them.

Detect

Incidents are flagged, or teams proactively research, hunt, and stress-test our systems

Investigate & Triage

Evaluate if incident is isolated or part of a broader trend on platform

Diagnose

Coordinate with teams on how incident bypassed our systems (e.g., filters, classifiers)

Intervene & Prevent

Action the incident and improve systems to prevent similar incidents in the future

Incident Management with Law Enforcement

TikTok has a specialized workflow to comply with U.S. Law Enforcement and regulatory agencies to process requests.

1	U.S. Law Enforcement submits user data request to TikTok through a webform available at: www.tiktok.com/legal/law-enforcement
2	The user data request enters a specialized queue to be processed by the Law Enforcement Response Team under U.S. Trust & Safety
3	U.S. Trust & Safety collaborates with Legal and Security teams to submit requested user data to U.S. Law Enforcement.

APP-329

Promoting Videos

APP-330

Video Promotion & Filtering

Promotion impacts fewer than 1% of videos. The selection process for promoted videos focuses on the criteria described below.
Filtering is meant to keep video quality high and the TikTok experience entertaining and engaging.

Promotion
Diversify Content
Support Creators
Tentpole Promotion
Music
Sponsored Promotion

Filtering – keep content engaging
QA (e.g. filter low quality, extremely short videos, extremely long videos)
Give new content a chance (e.g. include some low Video View ("vv") videos, include recent videos)
Include local content (e.g. 50% of content pool should be from U.S.)
Deduping (e.g. don't show same creator or audio repeatedly)
New User Feed (e.g. don't include duets, don't include non-U.S.)

Parameters are <u>NOT</u> Political

How Video Promotion and Filtering Works
(Note: Moderation Systems Not Shown for Simplicity of Diagram)

Content Pool

Content Partnerships — request →
Music — request →
Advertising — request →

U.S. Promotion Platform

Tag Content to be promoted (Teal color) →

Tagged content ranking increased
Filter

Recommendation Engine

Post-processing to further increase ranking when necessary
Filter

Business Rules

Business and Quality Goals

APP-332

Video
Promoted Video

26

Transparency

APP-333
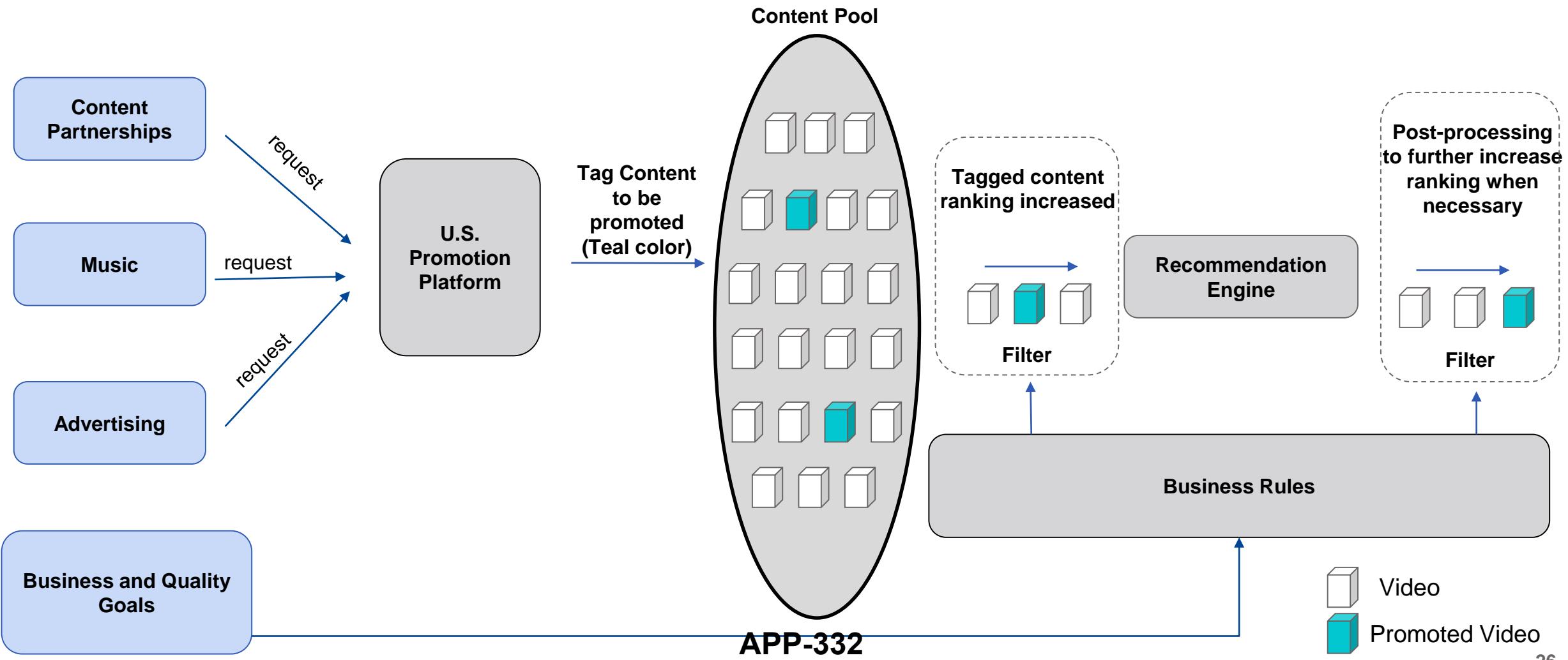
Transparency Reports & Centers

www.tiktok.com/transparency

Quarterly Transparency Reporting

Key Metrics Include:

- Total video removals by market
- Total video removals by reason
- Proactive removal rate and removal rate within 24 hours
- Law enforcement requests for user information
- Government requests for content restrictions
- Intellectual property removal requests

The next report will be published December 1, 2021.

Transparency & Accountability Center

Los Angeles
Washington D.C. (coming soon)
Dublin, Ireland (coming soon)

- **Candid Feedback:** Opportunity for observers to provide meaningful feedback on TikTok's practices

- **Content Moderation:** Opportunity see and evaluate how trained moderators apply policies to review technology-based actions

- **Data & Security**: Opportunity to learn about Cyber Defense, Security Assurance, and Data Protection programs

Conclusion and Q&A

The parties look forward to continuing to engage with CFIUS on each of these topics and to complete an NSA that fully resolves any U.S. national security concerns.

APP-335

Appendix

APP-336

Technical Explanation: The Recommendation Algorithm

The For You feed is part of what enables connection and discovery. It's central to the TikTok experience and where most of our users spend their time.

Logical Architecture

Raw Data

- Content Pool
- User Behavior

Offline Training

- Batch Training
- Featuring Engineering
- Batch Infra

Online Training

- Online Training
- Featuring Engineering
- Streaming Infra

Online Serving

- Rank
- Rough Sort
- Recall

Shared Inferred Data

- User Embedding
- Content Embedding
- Parameters for Models

Some Typical Model

- Predict: Stay Time
- Predict: Finish Rate

Stay Time Model

Like / finish / share / skip

⊗

- User embedding
- Video embedding

- Neural network
- Neural network

- User info
- Video info

Technical Explanation: Content Distribution

TikTok US

Behavior — Public Content & Metadata From US User

Content — Public Content & Metadata From US User / Protected Content & Metadata From US User

TikTok US Moderation System → TikTok US Recommendation Content Pool → TikTok US Recommendation System → TikTok US Content Distribution Strategy System

TikTok ROW

Content — Public Content & Metadata From ROW User / Protected Content & Metadata From ROW User

Behavior — Public Content & Metadata From ROW User

TikTok ROW Moderation System → TikTok ROW Recommendation Content Pool → TikTok ROW Recommendation System → TikTok ROW Content Distribution Strategy System

APP-338

Exhibit F

Redacted Version

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States

November 30, 2021

ByteDance Participants (telephonic)

- **Erich Andersen** – General Counsel and Head of Corporate Affairs
- **Vanessa Pappas** – TikTok Chief Operating Officer
- **Will Farrell** – TikTok Head of Global Cyber and Data Defense
- **Matt Penarczyk** – TikTok Head of Legal, Americas
- **Sarah Aleem** – TikTok Senior Legal Counsel, North America
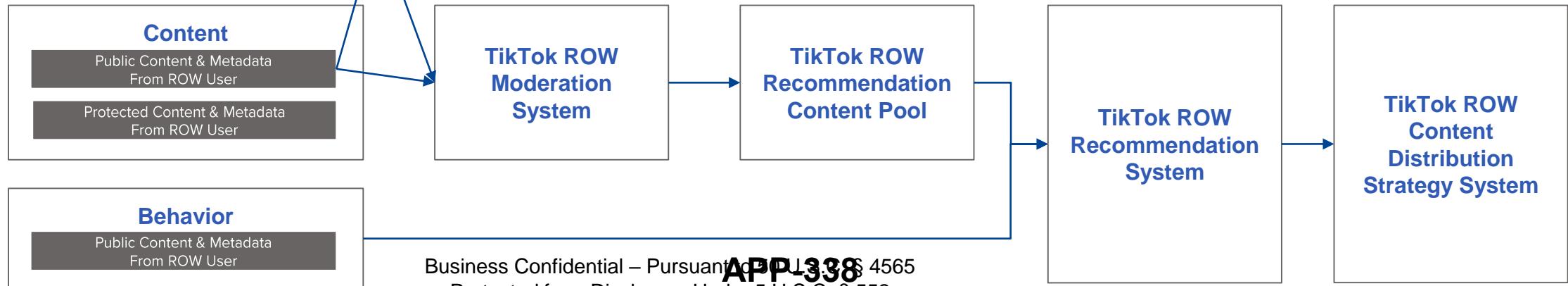- **Yufan Zhu** – Head of TikTok Engineering US

Oracle Participants (telephonic)

- **Edward Screven** – Chief Corporate Architect
- **Craig Stephen** – Senior Vice President, Research and Development
- **Scott Gaetjen** – Vice President, Cloud Chief Architect
- **Brian Higgins** – Senior Vice President, Legal

Counsel

- **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **Monty Roberson** (Covington) on behalf of ByteDance
- **Giovanna Cinelli** and **Christian Kozlowski** from Morgan Lewis on behalf of Oracle

APP-340
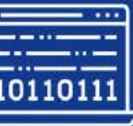
Topics for Today's Discussion

1	Key Principles
2	The TikTok Product Development Process & Code Lifecycle
3	Overview of the Oracle System
4	Role of the Dedicated Transparency Centers
5	Progress to Date on Building a System that Meets National Security Requirements

APP-341

Key Principles

	ByteDance continues to own its source code, but provides a trusted, auditable, and verifiable deployment of all production code for the TikTok App and TikTok Platform through the Oracle infrastructure and with Oracle validation and analysis.
	Provide one or more physical sites for source code analysis and review.
	Provide complete access and transparency to ALL TikTok source code for Oracle, the CMAs, and 3rd Party Source Code Inspector.
	The approach, process, and technology all need to operate at sufficient scale and speed to keep up with development and make sure U.S. users have feature/experience parity with the rest of the world.

APP-342

Overview of Source Code Development and Security Review Proposal

ByteDance provides access to ALL source code

→

Source Code enters Secure Enclave for analysis by the Trusted Technology Provider (TTP)

App →

Apple App Store

Google Play Store

Backend Services →

TTP
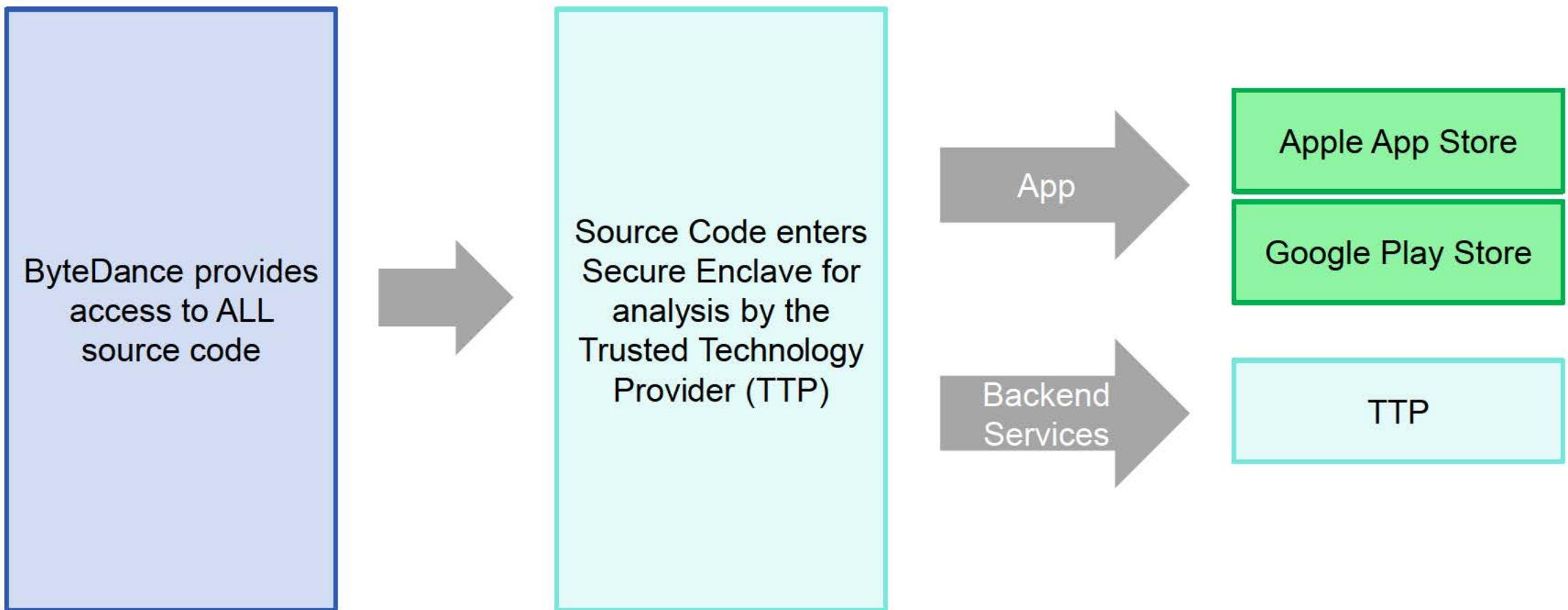
APP-343

Overview of TikTok Product Development Process

Version 1.0

Product Design → Privacy Review → Develop-ment → Testing → Release

1 week

Version 2.0

Product Design → Privacy Review → Develop-ment → Testing → Release

1 week

Product Development is constant. New features and updates are being released frequently, as illustrated by this diagram.

Version 3.0

Product Design → Privacy Review → Develop-ment → Testing → Release
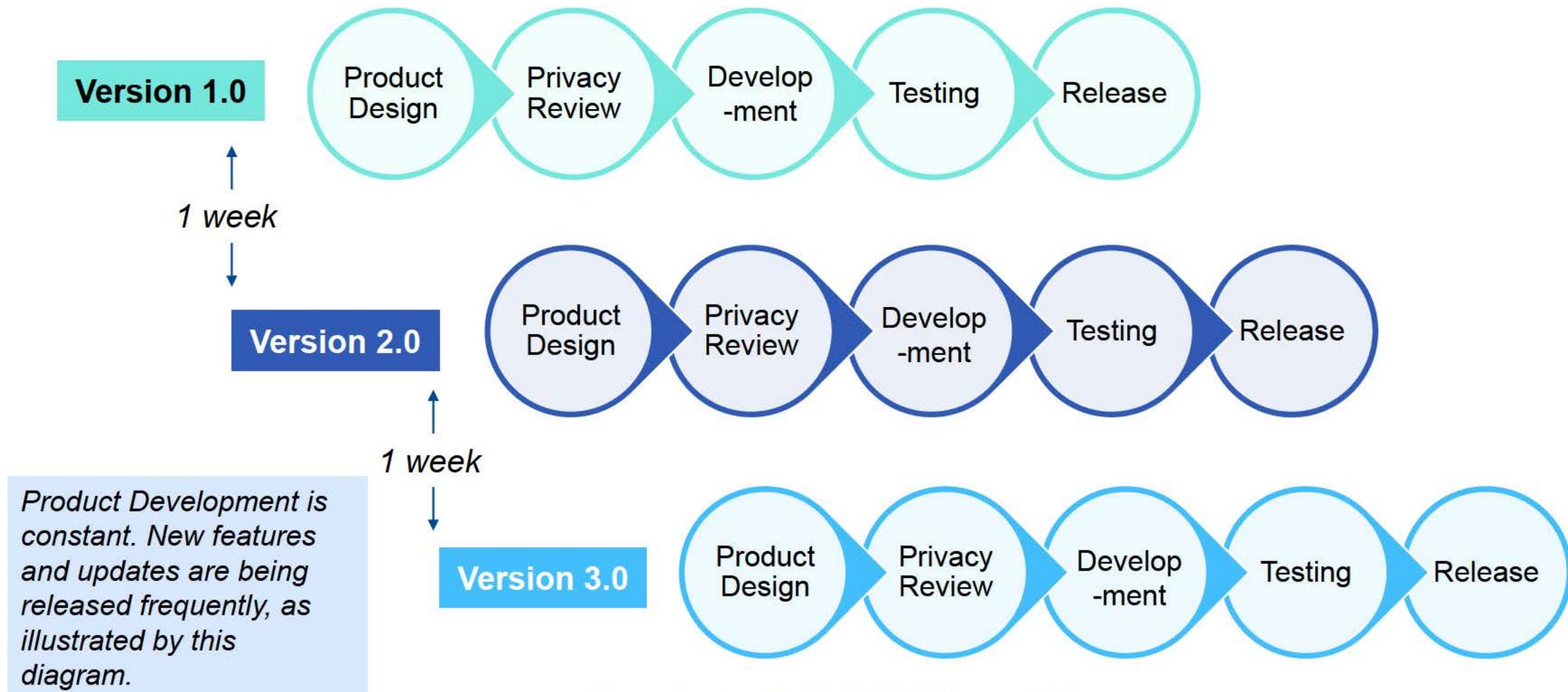
APP-344

TikTok Internal Tools, Systems & Tech Stack

End User (Client)	iOS		Android	Web
Data Center	Backend Services	Recommendation Engine	Advertising	Content Moderation
	Internal Tools	Collaboration · Content Mod Tools · Ticketing · Security Tools		
		300+ supporting apps / tools / services		
	Big Data Platform			
	Infrastructure			
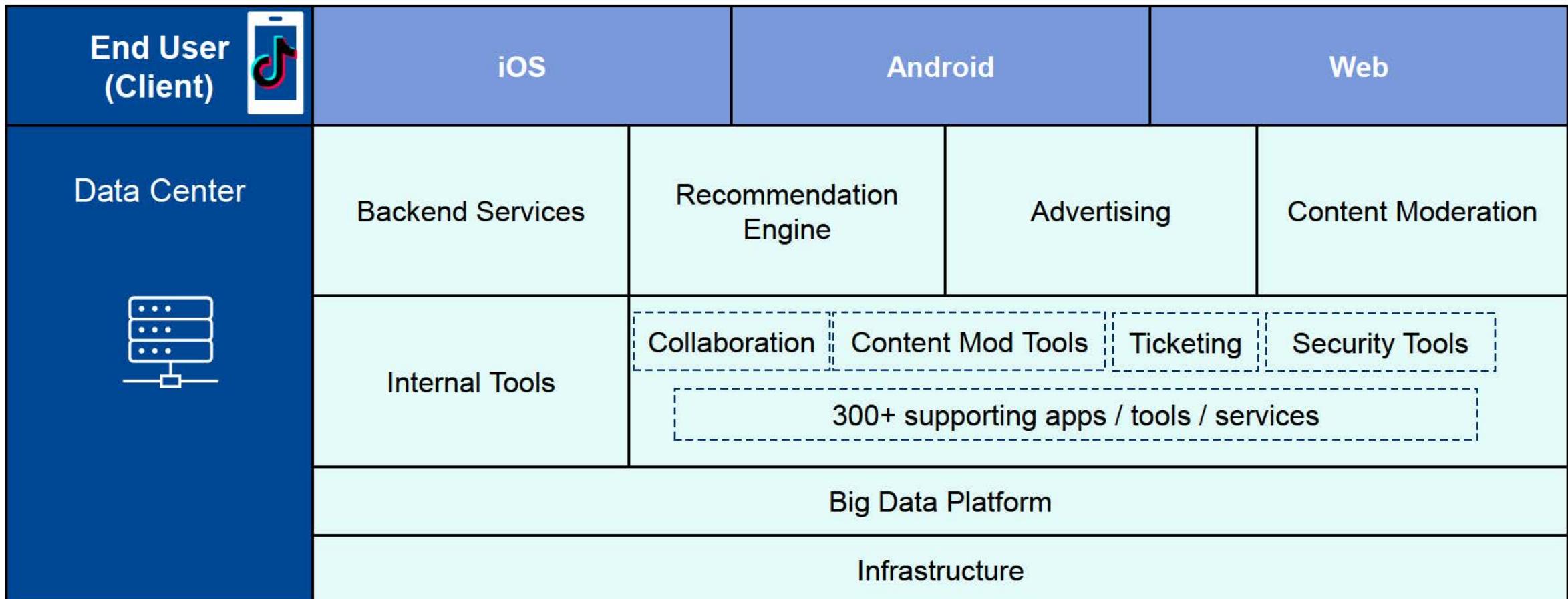
Note: All of the above are subject to code analysis by Oracle

APP-345

Oracle System Architecture Diagram

APP-346

Systems and Processes for Code Compilation and Production Code Security

Systems and Processes for Code Compilation and Production Code Security

1	**Develop**

a. TikTok develops new code and stores it in the **TikTok Codebase (includes Application Scripts & Component Build Events)**

2	**Synchronize**

a. The code is synchronize the source code from the **TT Codebase** with the **TT U.S. Ops Secure Codebase** within the **SCE**

APP-348

Systems and Processes for Code Compilation and Production Code Security

| 3 | **Source Code Security Review** |

a. **TTP** performs prioritized analysis and manual reviews of the source code from the **Dedicated Transparency Center ("DTC")**

b. **TTP** Security Analysts examine all aspects of the Source Code and Related Files to assess the presence of any vulnerabilities, including Malicious Code, that could affect the confidentiality, integrity, or availability of the TikTok App, TikTok U.S. Platform, or Protected Data

APP-349
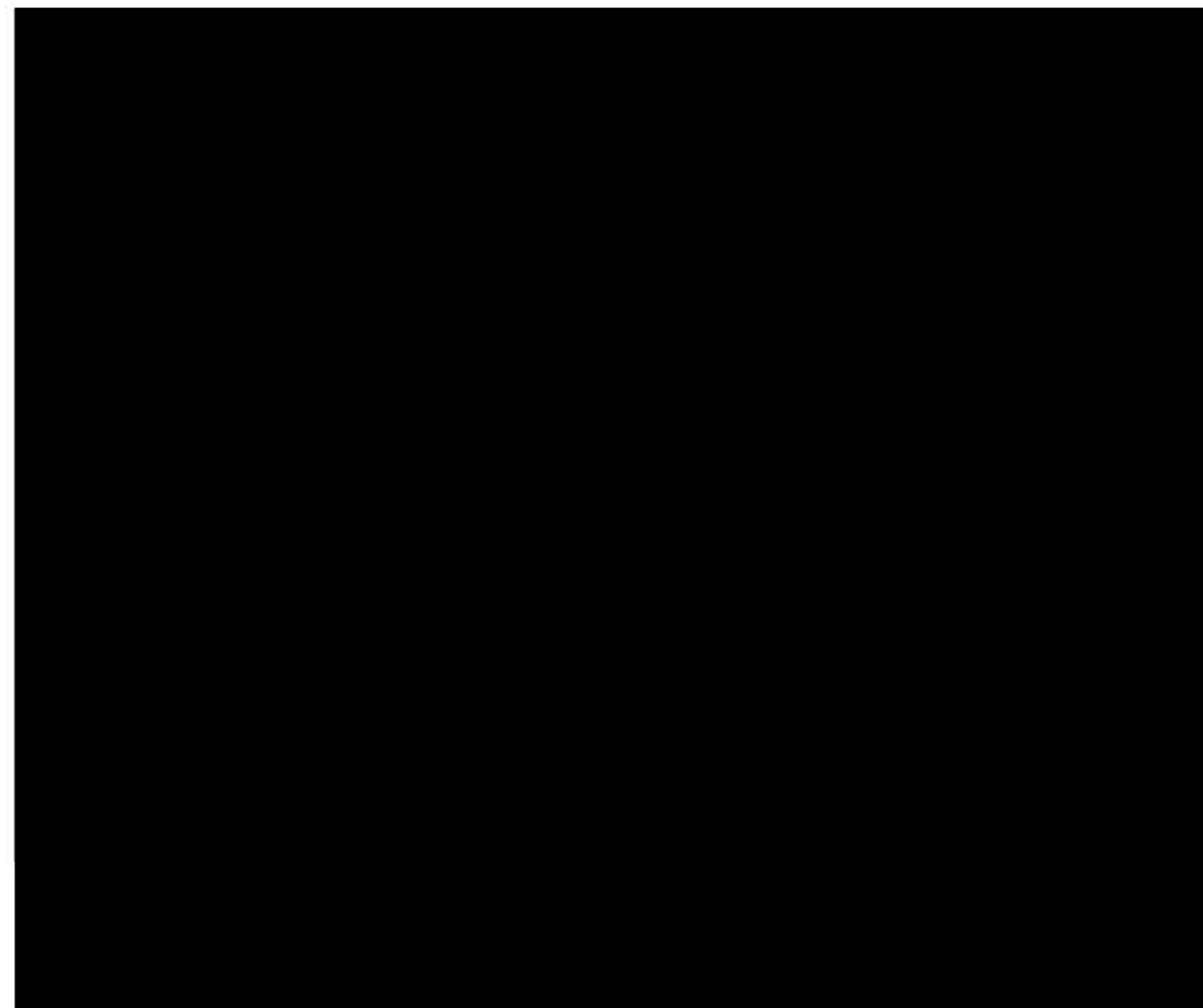
Systems and Processes for Code Compilation and Production Code Security

4a	**Compile (Mobile)**

a. TikTok U.S. Ops uses a **System Interface** to access **Components Build Management** from the **Sync Gateway** in the **SCE**

5a	**Deploy (Mobile)**

a. Oracle pushes **Application Scripts** from the **App Repository** to the **Mobile Deployment Gateway** within th Oracle Enclave within the **SCE Tenancy**

b. Oracle pushes **Application Scripts** from the **Mobile Deployment Gateway** to the **App Stores** on the **Internet**

APP-350

Systems and Processes for Code Compilation and Production Code Security

4b	Compile (Server)

a. TikTok U.S. Ops uses the **Build System Operations Gateway** within the **Secure Computing Environment ("SCE")** to access the **Building Pipeline** within the **SCE, which:**

- Compiles the server code, producing executable binaries and artifacts

- **Software Bill of Materials ("SBOM")** is generated. All artifacts are signed so the **TTP** can verify the code hasn't been modified post **TTP** Analysis

APP-351

12
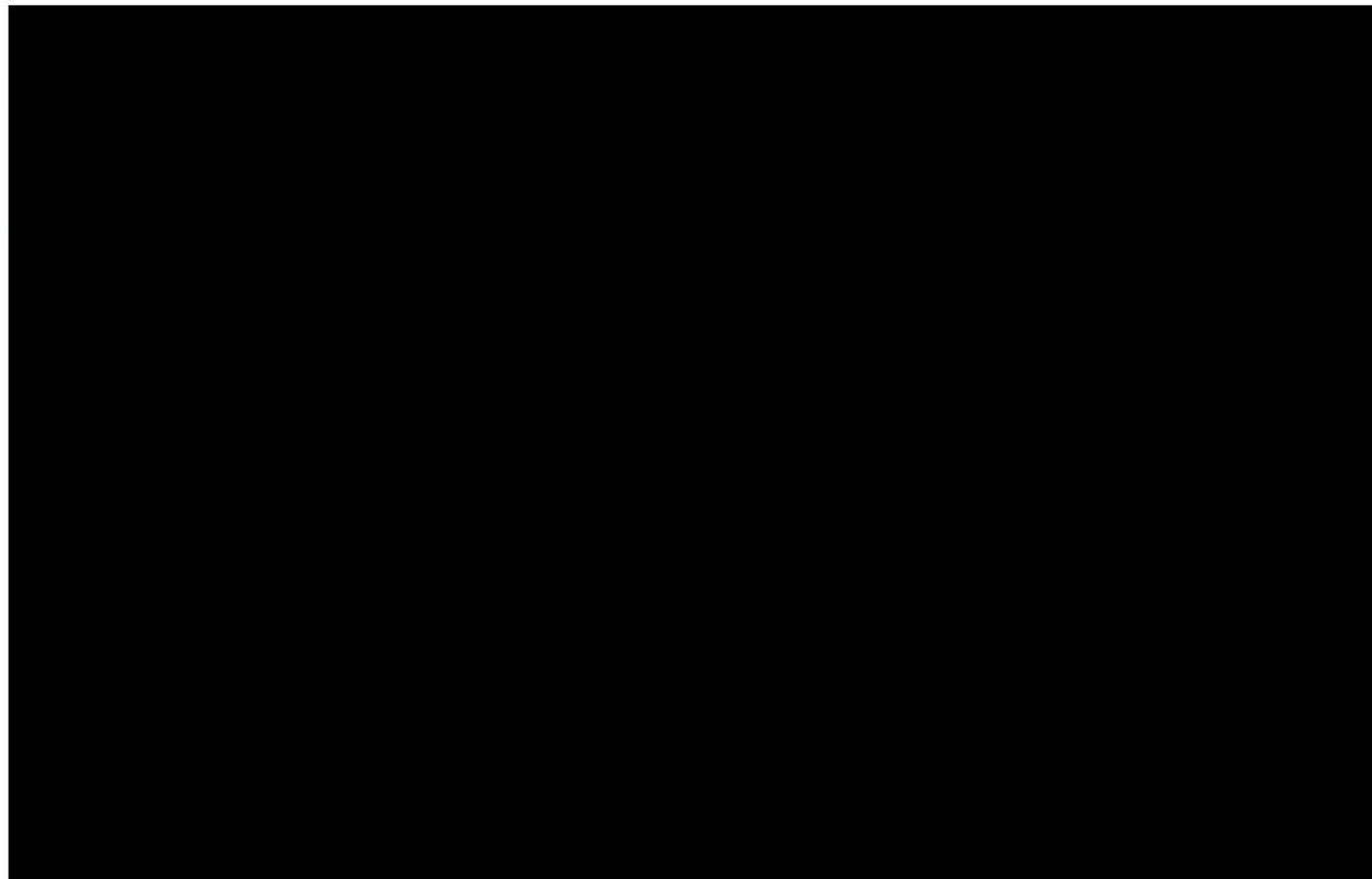
Systems and Processes for Code Compilation and Production Code Security

5b	Deploy (Server)

a. TikTok U.S. Ops triggers a deployment request. **Operations Gateway -> Deployment Platform**

b. **TTP** will be able to verify the build signature ensuring only approved code can be deployed.

c. TikTok U.S. Ops uses the **Deployment Platform** to deploy fully reviewed and approved compiled and executable binaries to the **TT Virtual Machine** (from approved base image)

APP-352
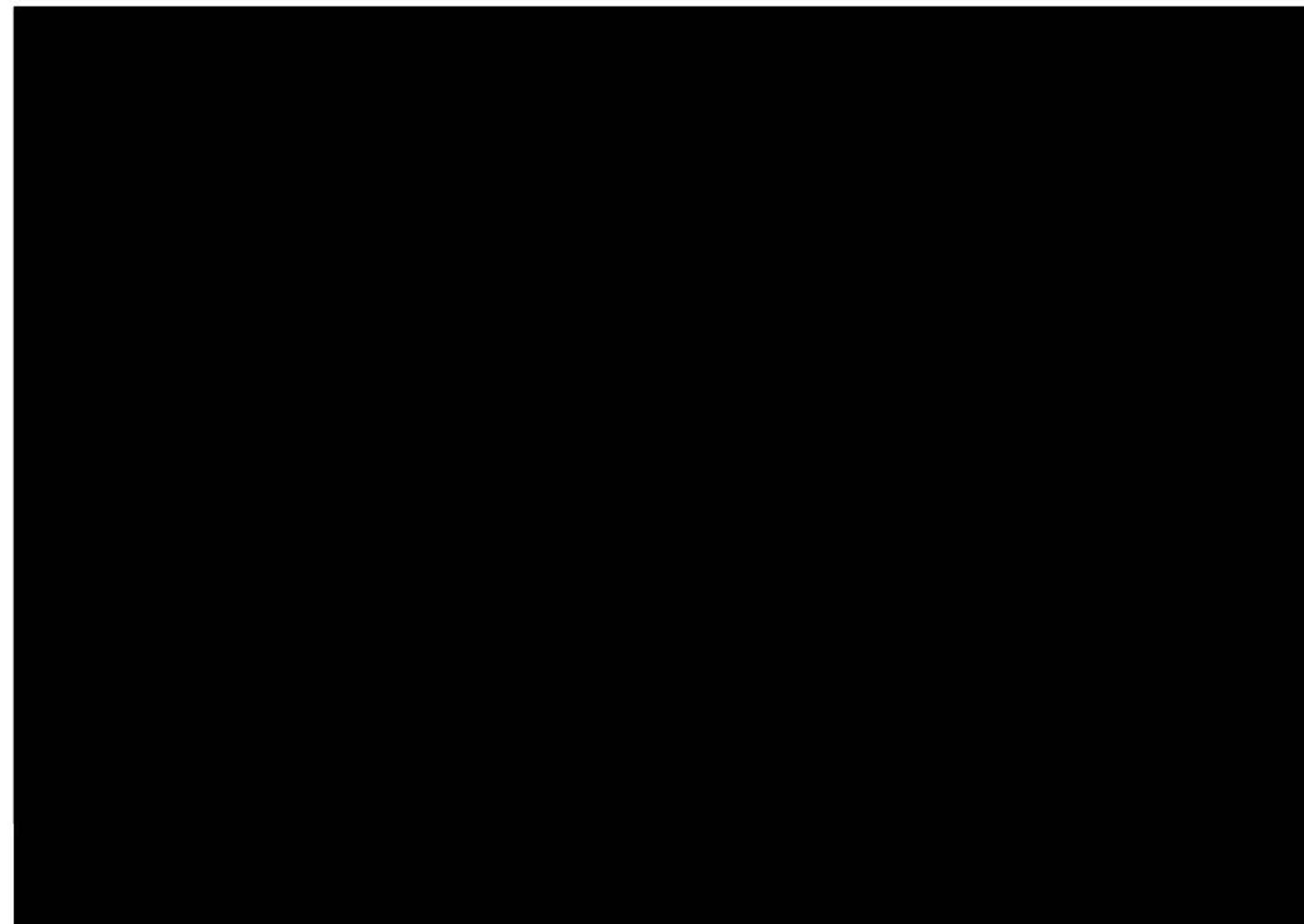
Systems and Processes for Code Compilation and Production Code Security

6	**Monitor**

a. **[Mobile] Oracle Mobile Sandbox** is used to monitor and control network communications of the TikTok mobile app

b. **[Server] The TTP Monitoring Agent** will be triggered once the new binaries have been deployed to the **TT Virtual Machines**. They will compare the checksum of the new binaries (found on the **SBOM**) against the checksum stored in the **Artifact Repository**

APP-353

14

Notional DTC Layout & Sites

We're moving forward with our first DTC Site and working with Oracle to identify other sites in parallel

- First site is under way at Union Market in Washington, D.C.
- Aligned with Oracle on workspace requirements (e.g. monitors, etc)
- Will have 2 separate network circuits
  - One dedicated and controlled by Oracle
  - Other will be TT US Ops, for access into the Secure Computing Environment (SCE) for Source Code access
- Space will be primarily occupied by Oracle and secured by TT US Ops
  - No ByteDance Employees in the space

APP-354
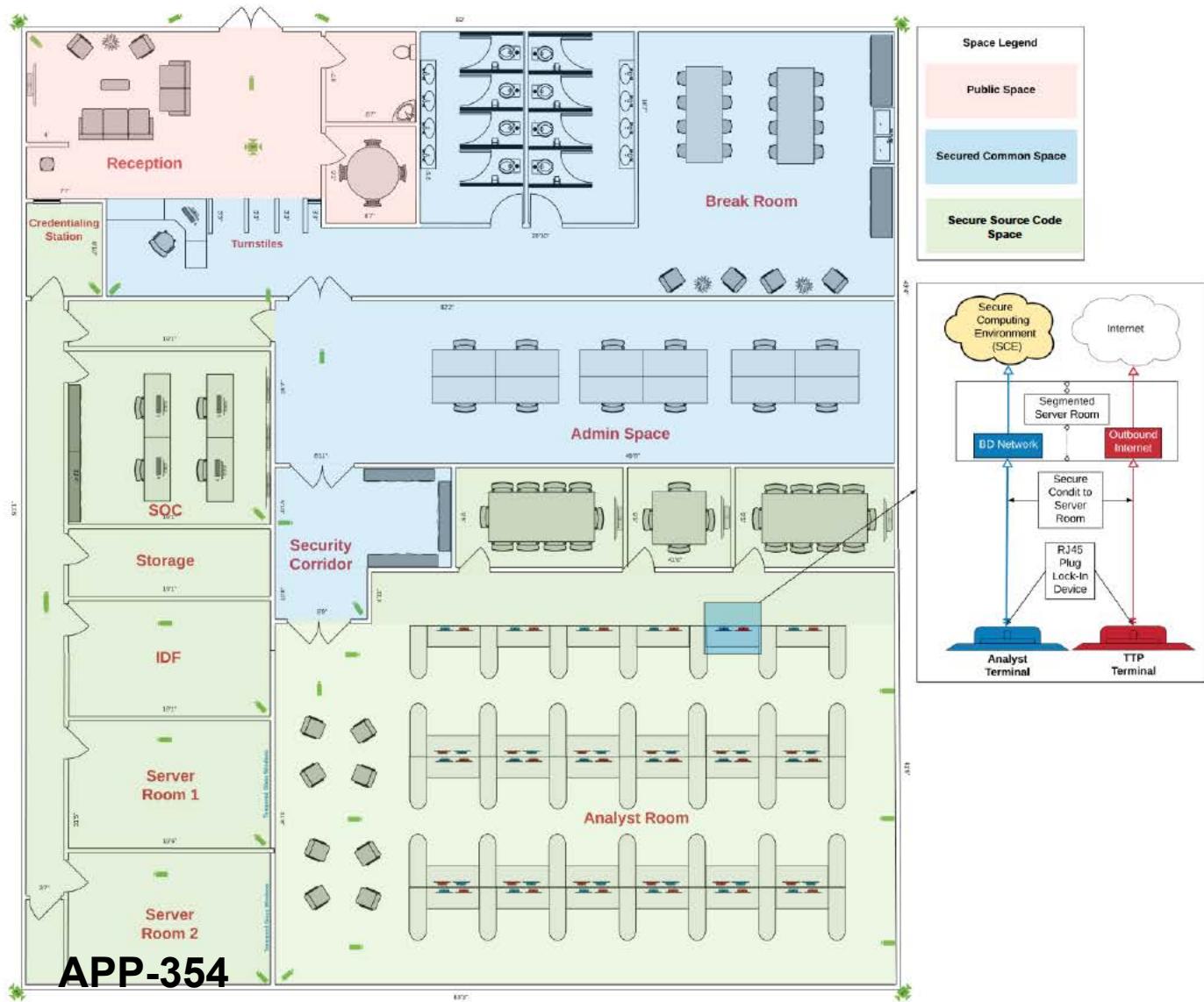
Oracle System Progress-to-Date

Oracle and ByteDance are working together on and compliance of TikTok U.S. Ops people, processes, and technologies. Collectively, the teams are preparing and conintuing to "move out" and get systems up and running.

Complete	In Flight	Next Steps
✓ 20,000 bare metal machines are now ready in the Oracle Enclave; this equates to 27,000 virtual hosts ✓ Up to 60% of U.S. user traffic is routing through Oracle Enclave to test reliability and performance	• Migration of 300+ apps • Establishing Secure Computing Environment • Initial operational gateway, data exchange system, app & third-party gateway (all currently in test)	• Continue to separate out the people and stand-up independent U.S.-based teams to sustain operations • Continue to build out and duplicate the environment in Oracle for failover for U.S. users to get the same reliability as Rest of World users

APP-355

Key Challenges & Pain Points

Hiring and scaling up TikTok U.S. Ops staff has been challenging due to the volume of headcount required and uncertainty around potential citizenship requirements

Typical stand-up of a longer-term, reliable, sustainable data center is 18 months; with a 9-month timeline, there are inevitable unknowns and reliability risks

Oracle must assess tens of millions of lines of code, requiring a balance of prioritizing code reviews in such a way that both gives Oracle and the CMAs comfort in quality while not delaying progress

Real estate (required in securing a DTC) processes are not typically fast and we are facing challenges due to uncertainty of final NSA terms, market-specific conditions and Covid-19 considerations

APP-356

Exhibit G

Content Assurance Process

Recommendation Engine

Purely algorithmic sorting based on a statistical model developed from behavioral signals from users in the community. Does not "understand" or reference a video's content.

- **TTP:** TTP conducts software inspection to confirm algorithm is not prioritizing or deprioritizing based on identification of content, but instead such actions are the result of content-neutral user behaviors.

Content Moderation

Hybrid (*i.e.*, machine & human) system to implement community guidelines that excludes content based on violations of community guidelines, IP infringement, and law enforcement requests.

- **TTP:** TTP conducts software inspection and testing/analysis to confirm the machine-implemented rules are linked to community guidelines and not unrelated content prioritization or deprioritization.
- **Content Advisory Council:** TTUSDS develops and publishes community guidelines in consultation with CAC.
- **TPM:** TPM provides ongoing review of community guidelines and—at the CAC's request—can review human exclusions of content are consistent with community guidelines.
- **TPA:** TPA includes review of content moderation implementation for consistency with stated guidelines; available to CMAs for interim audits if necessary.
- **TTUSDS:** Content moderation for the TikTok App that requires access to any Protected Data will be conducted by U.S.-based personnel under supervision of Security Committee.

Video Promotion and Filtering

Based on human decisions, TikTok undertakes software-based promotion and filtering of some videos to address commercial, product goals, and promote locally-based content to keep video feeds diverse and of appropriate quality.

- **TTP:** TTP conducts software inspection and testing/analysis to confirm functionality and how content is tagged for promotion or filtering.
- **TPM:** TTUSDS documents for the TPM how Video Promotion and Filtering functions; TPM/TPA can run periodic audits to ensure decisions are consistent with established processes and for commercial purposes.
- **TPA:** TPA includes review of video promotion and filtering for consistency with stated policies; available to CMAs for interim audits if necessary.
- **TTUSDS:** TTUSDS ensures only authorized personnel are engaged in Video Promotion and Filtering for TikTok App.

User & Outside Groups

- **Users and outside groups:** Users and other interested parties can view TikTok's User Agreements (*e.g.*, Privacy Policy, Terms of Service, content moderation policies and other published policies thereto) on the TikTok App, review TikTok's quarterly Transparency Reports, and visit the Transparency Center in TikTok's LA office.

APP-358

Exhibit H

December 28, 2022

The Honorable Wally Adeyemo
Deputy Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Deputy Secretary Adeyemo:

On behalf of ByteDance Ltd. ("ByteDance" or the "Company"), we are writing regarding the ongoing process of the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") in relation to TikTok and ByteDance's acquisition of Musical.ly.

We specifically request a meeting with the Deputies of the Committee as early as possible in the new year to affirm our client's commitment to finalize the National Security Agreement ("NSA") that has been pending before the Committee for five months — after having been negotiated in painstaking detail over the preceding nineteen months. If the Committee is not prepared to finalize the NSA, we request engagement with the Deputies so that we may be appropriately informed of the Committee's concerns and be allowed to address them.

For more than three years — since the Committee first approached ByteDance in 2019 regarding the Musical.ly acquisition — our client has sought at every turn to engage constructively with CFIUS, to be solutions-oriented, and to approach the Committee's process with respect and transparency. It has done so in the face of an extraordinary public campaign against it, against a process preceding the August 14, 2020 Executive Order that was totally untethered to the law, and despite the Committee's recent disengagement and apparent decision of the Administration to engage publicly rather than continue to work privately and constructively with the Company on a national security solution.

From January 21, 2020, until August 2022, our client and the agencies worked diligently and constructively — and in confidence — through the complex operations of the TikTok app and platform to develop an unprecedented, robust national security solution that could set the benchmark for U.S. leadership on security issues related to similar applications and platforms globally. The hallmarks of this solution include:

- **No data access from China**. All U.S. user data – including expatriate data – would be safeguarded in the U.S. under a special corporate structure (U.S. Data Security & Oracle).

- **All software code—app and backend—secured by a U.S. and U.S. Government-approved Trusted Technology Provider (*i.e.*, Oracle)**. The TikTok U.S. Platform and TikTok U.S. app will be deployed through Oracle infrastructure and subject to source code review/vetting by Oracle and another third party (the "Source Code Inspector") approved by CFIUS.

APP-360

- **<u>Content moderation transparency and compliance</u>**. There are multiple layers of protection to address concerns related to the content of the application, including ensuring that all algorithm/content moderation—both human and technical—is subject to third party verification and monitoring.

- **<u>Separation of the business responsible for the foregoing from China</u>**. The NSA requires a special board, with Security Directors subject to the U.S. Government's approval, to oversee TikTok U.S. Data Security, and in turn exclude ByteDance from such responsibilities. In addition, further separation between ByteDance and U.S. operations would be achieved through an additional board between TikTok U.S. Data Security and ByteDance (*i.e.*, TikTok Inc.) that again includes a U.S. Government-approved Security Director.

- **<u>Unprecedented layers of review, monitoring, and auditing including</u>**:

  o The Security Directors responsible for the TikTok U.S. Data Security governance structure (with a Security Director also on the board of TikTok Inc.);
  o The Trusted Technology Provider (Oracle);
  o A third-party monitor;
  o A third-party auditor;
  o Data deletion confirmation (*i.e.*, all historical U.S. user data deleted from ByteDance systems);
  o The Source Code Inspector; and
  o The CFIUS Monitoring Agencies.

- **<u>Strict penalties for noncompliance</u>**, including a possible "kill switch" (which would give CFIUS the explicit authority to suspend app service in the U.S.) and significant money penalties.

Our client's commitment to this historic solution is not simply rhetorical, as it has already invested more than $1 billion to advance the NSA's operationalization. These steps—to include the storage of all U.S. user data in the Oracle infrastructure—have been taken in good faith, and based on the positive engagement with CFIUS that occurred from January 21, 2020 through August 2022. In addition, the steps have been taken in consultation with and with the full support of ByteDance's majority shareholding, well-respected U.S. investors.

We note that the Company continues to take steps to advance the operationalization of this solution notwithstanding the significant politicization that has occurred over the last five months. The highly politicized rhetoric has been particularly disappointing given the Committee's lack of engagement with ByteDance since August 2022. As the Committee is aware, we submitted a near-final NSA on August 23, 2022, and have followed up proactively several times with additional information (including the identities of the proposed Security Directors), but, despite our requests, we have received no substantive updates or engagement from the Committee since that submission in August. This failure of process has been exacerbated by press reports on the government's

apparent ongoing deliberations and negative public comments from senior officials in the CFIUS process.[1] Respectfully, we do not believe such leaks and comments advance the resolution of national security interests, nor comport with the confidentiality requirements of the statute.

Our request for a meeting is made with the spirit and intent of completing the strong substantive blueprint developed by the interagency process and the Company over the previous last several years. Our focus, and that of our client, strongly remains in support of a solution to be finalized through constructive engagement with the Committee—and, again, it is for that reason that we seek a meeting.

Best regards,

By: _____

Michael E. Leiter
Skadden, Arps, Slate, Meagher &
Flom LLP
1440 New York Avenue, N.W.
Washington, DC. 20005-2111

By: _____

David Fagan
Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956

---

[1]   Lauren Hirsch, David McCabe, Katie Benner and Glenn Thrush, "TikTok Seen Moving Towards U.S. Security Deal, but Hurdles Remain," New York Times, September 26, 2022; Eric Tucker, "FBI director raises national security concerns about TikTok," AP News, December 2, 2022; "Treasury Secretary Janet Yellen on TikTok national security fears," 60 Minutes, available at cbsnews.com, December 9, 2022; Gavin Bade, "TikTok national security deal roiled by internal strife," Politico, December 16, 2022; Stu Wu, Kate O'Keefe, and Aruna Viswanatha, "TikTok Security Dilemma Revives Push for U.S. Control," Wall Street Journal, December 26, 2022.

Exhibit I

TikTok

February 25, 2023

The Honorable Wally Adeyemo
Deputy Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

The Honorable Lisa Monaco
Deputy Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Deputy Secretary Adeyemo and Deputy Attorney General Monaco:

I am writing regarding the ongoing process of the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") in relation to ByteDance Ltd.'s acquisition of Musical.ly, and the National Security Agreement ("NSA") governing TikTok's operations in the United States.

We remain committed to resolving this matter through an agreement with CFIUS. To that end, I request a meeting with you and, as you deem appropriate, other Deputies of the Committee to provide an update on the efforts that TikTok has made to implement the NSA that was diligently and constructively — and in confidence — negotiated with the Committee's national security professionals from 2020 through August 2022, and to finally bring this matter to closure. I also would like to offer a meeting with the CEO of TikTok, Shou Zi Chew, who will be in Washington between March 6-23.

While we believe that the NSA that was submitted in August 2022 is robust and should fully resolve the national security interests, if there are additional measures that you believe are necessary to address your concerns, we are keenly interested in hearing them, and I commit to you that we will do everything in our abilities to address those concerns. I also have asked our outside counsel to extend an invitation to your staff to visit the Dedicated Transparency Center ("DTC") that we established in Maryland where Oracle is currently testing our code, consistent with the commitments in the NSA.

For more than three years — since the Committee first approached ByteDance in 2019 regarding the Musical.ly acquisition — we have sought at every turn to engage constructively with CFIUS, to be solutions-oriented, and to approach the Committee's process with respect, transparency, and confidentiality. We have done so because we believe that we share a common objective with the Committee: to ensure the safety of TikTok's U.S. users and the integrity of our platform and app, including against misinformation campaigns. We have done so notwithstanding

APP-364

♪ TikTok

that ByteDance grew TikTok organically, not through the acquisition of the Chinese-owned Musical.ly and its limited assets that are virtually irrelevant to TikTok today. And we have done so in the face of an extraordinary public campaign against us, and against a process preceding the August 14, 2020, Executive Order that was untethered to the law.

At all times, we also have been fully respectful of the important CFIUS process. We have been responsive when the Committee has posed questions; we have been proactive in bringing issues to the attention of the Committee; we have been constructive in proposing solutions; and we have been patient as the Committee has deliberated. In this light, we have been increasingly dismayed by the Committee's lack of engagement over the last six months. This has been made worse by the public commentary from senior Administration officials, and we were particularly disappointed to see public statements from the Deputy Attorney General that unfairly and inaccurately portray TikTok in a negative light.[1] We recognize that the public campaign being run against us also puts pressures on the agencies, but we equally — and firmly — believe that the path forward should be predicated on constructive, substantive, and fact-based work on a national security solution.

Despite the lack of engagement from the Committee, we have continued voluntarily to implement our proposed solution, at a cost of more than $1 billion to our company — a solution that will address the risks that are being publicly cited, namely the risks posed by Chinese law. U.S. user data and the TikTok U.S. app and platform will be in the cloud environment of the Trusted Technology Provider (*i.e.*, Oracle), and control over such data and systems will be in the hands of TikTok U.S. Data Security, managed by U.S. persons approved by CFIUS, and overseen by a board of security experts who owe a duty to protect U.S. national security. Further, as noted, we have already established a DTC, as proposed in the NSA, for the express purpose of enabling security inspections, reviews, and verification of TikTok Source Code and Related Files. We invite the agencies to visit the DTC, now up and running in Maryland, to understand how much progress our company has made in this effort and of course to offer their suggestions for any enhancements that they feel will be necessary to address the U.S. government's interests.

I ask that we work together to return to engaging on a solution. I firmly believe that we share the common interest in protecting the security of our users and in preserving their freedom of expression and thought, without interference by any government. I would welcome the opportunity to meet in person to advance that common interest, and to introduce you to TikTok's CEO, Shou Zi Chew.
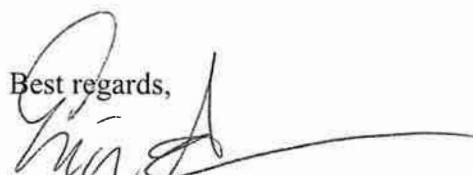
Best regards,

Erich Andersen
General Counsel – ByteDance and TikTok

---

1 Hannah Rabinowitz, "US deputy attorney general: 'I don't use TikTok, and I would not advise anyone to do so'" CNN, February 16, 2023. ("Any company doing business in China for that matter is subject to Chinese national security laws, which requires turning over data to the state, and there is a reason we need to be very concerned.... The bottom line is that China has been quite clear that they are trying to mold and put forward the use and norms around technology that advance their privilege and their interests.... Their interests, which are not consistent with our own. Their interests, which are fueled by and directed toward an authoritarian approach to their government. And that is not consistent with ours." Because of those concerns, Monaco said: "I don't use TikTok, and I would not advise anyone to do so.")

Exhibit J

From: Leiter, Michael E (WAS) [Michael.Leiter@skadden.com]
on behalf of   Leiter, Michael E (WAS) <Michael.Leiter@skadden.com> [Michael.Leiter@skadden.com]
Sent: 3/17/2023 10:30:23 PM
To: Brian.Reissaus@treasury.gov; Andrew.Fair@treasury.gov; Devin.DeBacker@usdoj.gov; Evan.Sills@usdoj.gov;
           Tyler.Wood@usdoj.gov; Winnie.Tsang@treasury.gov; Sarah.Oldham@treasury.gov; David.Newman2@usdoj.gov;
           Eric.S.Johnson@usdoj.gov
CC: dfagan@cov.com; Theodore.Posner@treasury.gov; Nayla.Kawerk@treasury.gov
Subject: RE: [Ext] RE: CFIUS Case. No. 20-100: Call & Meeting Request

Brian,

Thank you for your note and we appreciate your views. We remain committed, as we have for more than three years, to a substantive discussion to reach a negotiated settlement and ultimately we will meet with those that CFIUS deems its lead agencies and—we hope—with those who have statutory authority and (according to Assistant Secretary Rosen's statements) have made the decision presented on March 6th. Thus we are happy to meet with staff-level officers from Treasury and Justice and, as noted in our email, we are prepared for both a phone call and an in person meeting to advance discussions.

While committed to constructive and substantive engagement, we also must state that we find implausible your statement that "[t]he Warner bill to which [we] refer is not tied to the present negotiations," which seems in tension with the explanation that we received on March 6th. In explaining the government's position in our meeting on March 6th, Assistant Secretary Rosen said, among other things, that the U.S. government concerns with this specific transaction arise against a backdrop of fundamental concerns around data security, particularly with respect to Chinese social media apps in the United States and Congressional scrutiny as seen in various legislative proposals. In addition, he noted that "some of [these proposals] have momentum" and that one or more may be enacted. Again paraphrasing, he said that there appears to be broad bi-partisan support to remove ByteDance ownership and concerns with data traveling back to China and "feeding ByteDance algorithms" and congressional proposals include unilateral authority to remove TikTok in the United States. Notably, while there was a clear reference to Congressional proposals, there was not a single reference to Section 721 in the statement.

Perhaps we were mistaken, but we came away from that meeting with the clear impression—based on the statements provided to us—that the potential legislation informed the government's position. That impression was reinforced when the next day the Warner legislation was introduced and near simultaneously, the National Security Advisor provided the Administration's endorsement of the legislation. Moreover, a litany of public reporting has associated the legislation with the Administration's CFIUS review of TikTok, and Senator Warner himself has linked the legislation to the CFIUS process and the Administration's new position.

We very much look forward to our discussions and hope and trust that they will be approached with a spirit of sincerity, candor, and confidentiality from the government. In the meantime, we will await your scheduling preferences that we will of course seek to accommodate. We would note that ByteDance's General Counsel will be flying on Friday so ideally we would have a call on Thursday afternoon.

Best,

David & Mike

Michael E. Leiter
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
1440 New York Avenue, N.W. | Washington | D.C. | 20005-2111
O: +1.202.371.7540 | M: +1.202.580.9111
michael.leiter@skadden.com

APP-367

From: Brian.Reissaus@treasury.gov <Brian.Reissaus@treasury.gov>
Sent: Thursday, March 16, 2023 10:00 PM
To: Leiter, Michael E (WAS) <Michael.Leiter@skadden.com>; Andrew.Fair@treasury.gov; Devin.DeBacker@usdoj.gov; Evan.Sills@usdoj.gov; Tyler.Wood@usdoj.gov; Winnie.Tsang@treasury.gov; Sarah.Oldham@treasury.gov; David.Newman2@usdoj.gov; Eric.S.Johnson@usdoj.gov
Cc: dfagan@cov.com; Theodore.Posner@treasury.gov; Nayla.Kawerk@treasury.gov
Subject: [Ext] RE: CFIUS Case. No. 20-100: Call & Meeting Request

Mike and David,

Representatives of Treasury and Justice would be pleased to meet with you and your client in the coming days to discuss a path forward in light of the government's position laid out on our March 6 call. As we discussed, the basis for our discussion will be the principles and frameworks for a viable resolution as generally summarized on that March 6 call. We are prepared to hear your proposals, questions, and discussion points on the topics listed in your email.

As for participation, the government will continue to be represented by Treasury and Justice – the co-leads in this matter. The Warner bill to which you refer is not tied to the present negotiations, nor does the proposed role for the Secretary of Commerce under that bill warrant changing the government participants in this discussion with you. We will continue to keep the other members of the interagency (including Commerce) informed and engaged, as we have been doing consistently throughout our engagement with you, and at the right time, and as and if needed, broaden out our discussions. However, at this time we do not intend to alter the government's participation for the next meeting.

We are still trying to deconflict our schedules, but are narrowing in on next Thursday or Friday. If there are times those days that do not work on your end please let us know. Otherwise, we will let you know once we identify times that work those days for the call.

Best,
Brian

From: Leiter, Michael E <Michael.Leiter@skadden.com>
Date: March 15, 2023 at 12:11:04 PM EDT
To: Reissaus, Brian <Brian.Reissaus@treasury.gov>, Fair, Andrew <Andrew.Fair@treasury.gov>, Devin.DeBacker@usdoj.gov <Devin.DeBacker@usdoj.gov>, Evan.Sills@usdoj.gov <Evan.Sills@usdoj.gov>, Tyler.Wood@usdoj.gov <Tyler.Wood@usdoj.gov>, Tsang, Winnie <Winnie.Tsang@treasury.gov>, Oldham, Sarah <Sarah.Oldham@treasury.gov>, David.Newman2@usdoj.gov <David.Newman2@usdoj.gov>, Johnson, Eric <Eric.S.Johnson@usdoj.gov>
Cc: dfagan@cov.com <dfagan@cov.com>, Posner, Theodore <Theodore.Posner@treasury.gov>, Kawerk, Nayla <Nayla.Kawerk@treasury.gov>
Subject: RE: CFIUS Case. No. 20-100: Call & Meeting Request

** Caution: External email. Pay attention to suspicious links and attachments. Send suspicious email to suspect@treasury.gov **

APP-368

Brian,

Per your request please find our proposed agenda below.

1. <u>Source Code</u>: timing and operational challenges to maintain globally integrated platform and export control issues
2. <u>Ownership</u>: potential structures and governance
3. <u>TTP</u>: USG vision for the role of the TTP in light of new CFIUS requirements and August 2022 NSA
4. <u>Proxy/Trust</u>: discussion of USG-rejected options not previously discussed
5. <u>Next steps</u>: group discussion

We also reiterate our request for Commerce to participate given the Administration's tying of the CFIUS negotiations with Commerce's potential related authority, as reflected by the near-simultaneous statement by the Assistant to the President for National Security Affairs supporting legislation introduced by Senator Mark Warner and your call with us announcing the new CFIUS requirements. We would further note that the Department of Commerce, as a statutory member of CFIUS, has current responsibility for any position taken by the Committee. Finally, with respect to an in person meeting Erich Andersen will be available Tuesday through Thursday next week. If such a meeting won't work, he may also be available in Washington the first week of April.

Best,

David & Mike

From: Brian.Reissaus@treasury.gov <Brian.Reissaus@treasury.gov>
Sent: Tuesday, March 14, 2023 10:53 PM
To: Leiter, Michael E (WAS) <Michael.Leiter@skadden.com>; Andrew.Fair@treasury.gov; Devin.DeBacker@usdoj.gov; Evan.Sills@usdoj.gov; Tyler.Wood@usdoj.gov; Winnie.Tsang@treasury.gov; Sarah.Oldham@treasury.gov; David.Newman2@usdoj.gov; Eric.S.Johnson@usdoj.gov
Cc: dfagan@cov.com; Theodore.Posner@treasury.gov; Nayla.Kawerk@treasury.gov
Subject: [Ext] Re: CFIUS Case. No. 20-100: Call & Meeting Request

Mike and David,

Thank you for following up, DOJ and Treasury can be available for a call to discuss next steps. While we figure out our availability, could you please provide us a list of topics/questions that you would like to discuss in advance of the call so that we can be in the best position to provide guidance on next steps.

Regarding your request for an in person meeting next week, following the call we will confer internally to coordinate timing and attendance.

Best,
Brian

From: Leiter, Michael E <Michael.Leiter@skadden.com>

Date: March 14, 2023 at 10:05:46 AM EDT
To: Reissaus, Brian <Brian.Reissaus@treasury.gov>, Fair, Andrew <Andrew.Fair@treasury.gov>, 'DeBacker, Devin (NSD)'
<Devin.DeBacker@usdoj.gov>, Evan.Sills@usdoj.gov <Evan.Sills@usdoj.gov>, Tyler.Wood@usdoj.gov
<Tyler.Wood@usdoj.gov>, Tsang, Winnie <Winnie.Tsang@treasury.gov>, Oldham, Sarah
<Sarah.Oldham@treasury.gov>, 'David.Newman2@usdoj.gov' <David.Newman2@usdoj.gov>, Johnson, Eric
<Eric.S.Johnson@usdoj.gov>
Cc: dfagan@cov.com <dfagan@cov.com>
Subject: CFIUS Case. No. 20-100: Call & Meeting Request

** Caution: External email. Pay attention to suspicious links and attachments. Send suspicious email to
suspect@treasury.gov ******

<div align="right">

Business Confidential - Pursuant to 50 U.S.C. Section 4565
Protected from Disclosure Under 5 U.S.C. Section 552

</div>

Colleagues,

As follow up to our call with Treasury and Justice CFIUS leadership on March 6th, we would like to schedule a call with
this group for Thursday or Friday of this week to discuss next steps. Ideally, we would prefer a time in the morning or
early afternoon so that ByteDance's General Counsel, Erich Anderson, can join given he is in London this week. In
addition, we would also like to schedule an in person meeting the week of March 20th when Erich is in Washington. For
both these discussions, we also ask—given the legislation supported by the Biden Administration and its involvement in
CFIUS—that appropriate Department of Commerce leadership (*e.g.*, Grant Harris) participate.

Best and thanks,

David & Mike

Michael E. Leiter
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
1440 New York Avenue, N.W. | Washington | D.C. | 20005-2111
O: +1.202.371.7540 | M: +1.202.580.9111
michael.leiter@skadden.com

===

APP-370

APP-371

Exhibit K

To: Brian.Reissaus@treasury.gov[Brian.Reissaus@treasury.gov]; Andrew.Fair@treasury.gov[Andrew.Fair@treasury.gov];
Devin.DeBacker@usdoj.gov[Devin.DeBacker@usdoj.gov]; Evan.Sills@usdoj.gov[Evan.Sills@usdoj.gov];
Tyler.Wood@usdoj.gov[Tyler.Wood@usdoj.gov]; Winnie.Tsang@treasury.gov[Winnie.Tsang@treasury.gov];
Sarah.Oldham@treasury.gov[Sarah.Oldham@treasury.gov]; David.Newman2@usdoj.gov[David.Newman2@usdoj.gov];
Eric.S.Johnson@usdoj.gov[Eric.S.Johnson@usdoj.gov]; Nayla.Kawerk@treasury.gov[Nayla.Kawerk@treasury.gov];
Theodore.Posner@treasury.gov[Theodore.Posner@treasury.gov]
Cc: Michael.Leiter@skadden.com[Michael.Leiter@skadden.com]
From: Fagan, David[dfagan@cov.com]
Sent: Thur 4/27/2023 11:13:29 PM (UTC)
Subject: [Ext] RE: CFIUS Case. No. 20-100: Status

Business Confidential - Pursuant to 50 U.S.C. Section 4565; Protected from Disclosure Under 5 U.S.C. Section 4565

Treasury and DOJ colleagues -

We wanted to provide the Committee with an update on the work that ByteDance has been undertaking to address the issues that we discussed in our meetings on March 6 and March 23. As we have discussed, both the Committee's position on ownership and its articulated position on source code raise extremely complex commercial and legal challenges. Nevertheless, ByteDance has been exploring solutions to both issues. There are active workstreams ongoing with the goal of being able to make a presentation to CFIUS later in May on potential solutions. To be sure, that does not mean that ByteDance agrees with the articulated positions, or that a divestiture or source code migration will even be practical commercially or because of the restrictions of Chinese law. It does mean, however, that ByteDance is working on the issues in good faith, and intends to present proposals on each prong in May. We currently think that will likely be the middle-to-latter half of the month, but will keep you apprised.

Best regards,

Mike and David

David Fagan

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5291 | M + 1 703 967 6940
dfagan@cov.com
www.cov.com

COVINGTON

Exhibit L

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States

May XX, 2023

ByteDance Participants

- **Erich Andersen** – General Counsel
- **Will Farrell** – Interim lead of Security for TikTok USDS

Counsel

- **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **Monty Roberson** (Covington) on behalf of ByteDance

APP-375

Current Situation: Opposing Views

CFIUS: "Divestiture and Source Code Migration"	Statement of Chinese Government Officials
◆ WSJ NEWS EXCLUSIVE | TECH	BUSINESS
U.S. Threatens Ban if TikTok's Chinese Owners Don't Sell Stakes	**China Says It Opposes Forced Sale of TikTok**
TikTok says forced sale won't resolve national-security issues; CEO set to appear before Congress next week	Biden administration demands that video app divest itself from its Chinese parent or face a U.S. ban
By John D. McKinnon [Follow]	*By Raffaele Huang* [Follow]
Updated March 15, 2023 6:45 pm ET	Updated March 23, 2023 9:09 am ET
https://www.wsj.com/articles/u-s-threatens-to-ban-tiktok-if-chinese-founder-doesnt-sell-ownership-stake-36d7295c	https://www.wsj.com/articles/china-says-it-opposes-a-forced-sale-of-tiktok-1a2ffc62

APP-376

Current Governance Offering

ByteDance Ltd.

TikTok Inc.

Board of Directors

| TikTok Inside Director | TikTok Inside Director | TikTok Outside Director | TikTok Outside Director | Chairperson of TikTok USDS Board |

100%
Financial ownership

TikTok U.S. Data Security Inc.
Wholly owned subsidiary of TikTok Inc.

Board of Directors / Security Committee

| Outside Director | Outside Director | Outside Director / Chairperson |

We've committed to the following:

- Shift all CFIUS Functions to USDS
- USDS Independent Board
  - All outside directors, no ByteDance/TikTok directors
  - All Directors must be approved by CFIUS
  - No reporting lines to ByteDance and TikTok
  - Fiduciary responsibility will be to the CFIUS
- TikTok Inc. Board:
  - Will include the USDS Chair
  - Majority outside directors
- USDS Personnel
  - Key Personnel subject to approval by CFIUS
  - All USDS Personnel subject to approved CFIUS Hiring Protocol

Furthermore, we're delivering on these commitments:

- USDS formed as a Delaware Corporation
- 1,500 employees already employed by USDS with open positions for another 500 to be hired by end of 2023
- Core CFIUS Functions have been transferred into USDS except for HR and Legal

APP-377

Additional Ownership Steps for Discussion

ByteDance Ltd.

↓

TikTok Inc.
Board of Directors

TikTok Inside Director	TikTok Inside Director	TikTok Outside Director	TikTok Outside Director	Chairperson of TikTok USDS Board

↓

TBD

↓

TikTok U.S. Data Security Inc.
Board of Directors / Security Committee

Outside Director	Outside Director	Outside Director / Chairperson
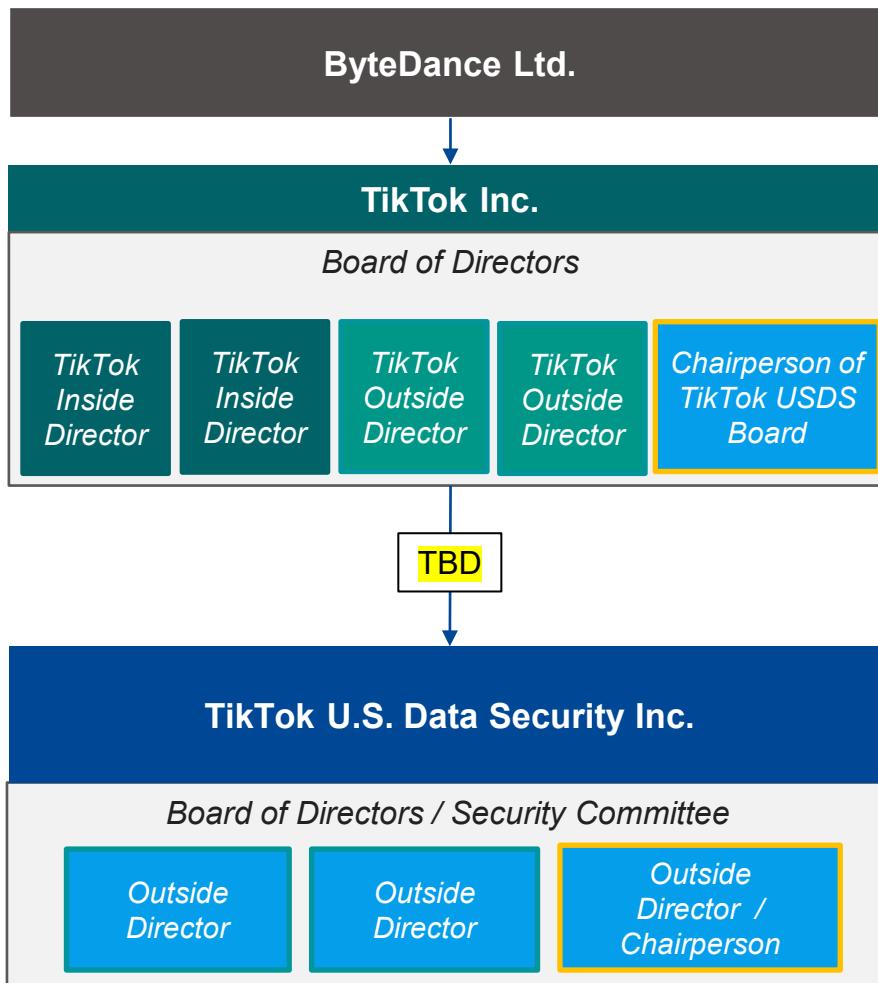
Challenges to Ownership Change of USDS

- Economic implications for shareholders and employees
- Change of control may impact existing agreements with third parties (e.g. music)
- Ownership of intellectual property
- USDS becomes de facto vendor to Global TikTok
- Regulatory approvals

Reminder: Challenges to Ownership Change of TikTok Inc.

- Not expected to receive regulatory approval ("forced sale" of business)
- Breaks global integration of non-national security business functions, such as sales and marketing
- Breaks interoperability (U.S. becomes a TikTok "island")
- Significantly increases business costs through duplication of roles and systems

Overall Challenges

- Even if the challenges above were overcome, it is not clear whether there are any potential buyers who could take on a U.S. TikTok business without ByteDance having some stake and supporting the application
- The effect of these challenges can result in an effective ban and impact 150 million Americans

APP-378

Overview of Source Code Migration Proposal

1	Brief review of current software assurance commitments and proposed enhancements
2	High level overview of TikTok technology stack
3	Drill down on technology relevant to content assurance
4	Company proposal for migration
5	Timing and risk factors
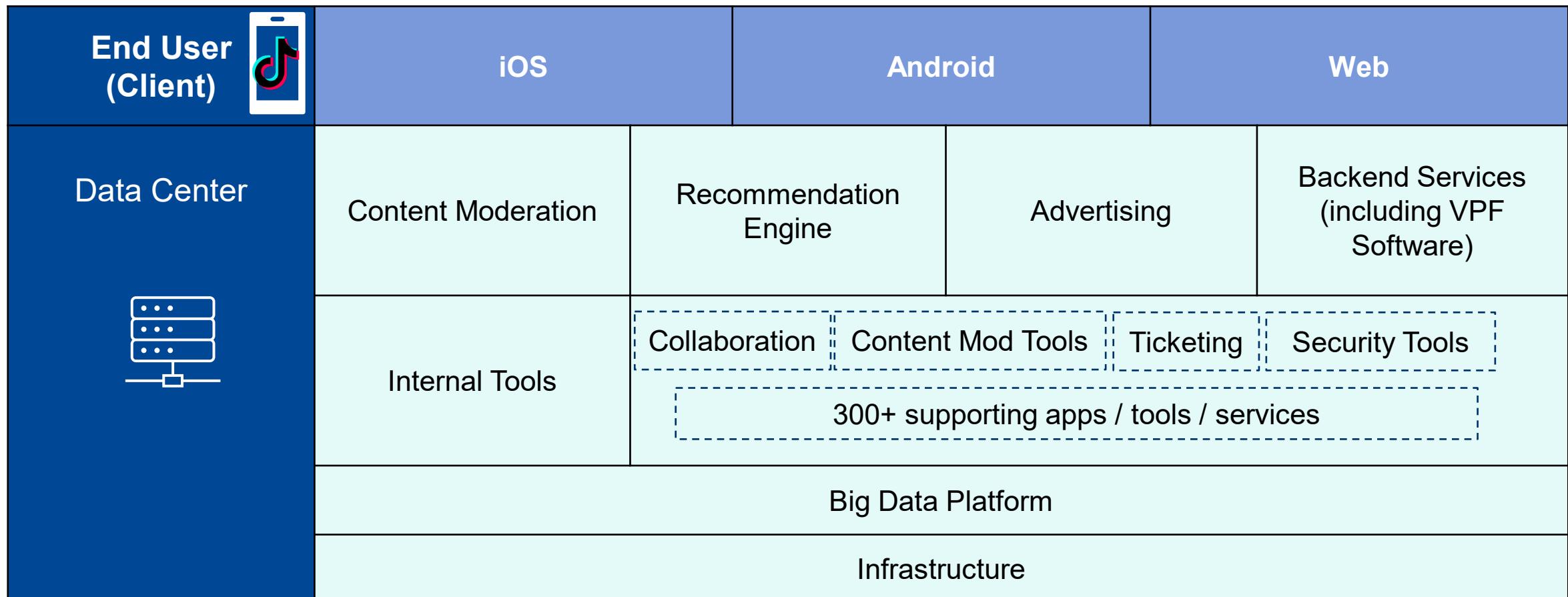
APP-379

High Level Stack View of TikTok Systems

End User (Client)	iOS	Android	Web
Data Center	Content Moderation	Recommendation Engine	Advertising	Backend Services (including VPF Software)

Internal Tools	Collaboration	Content Mod Tools	Ticketing	Security Tools
	300+ supporting apps / tools / services	
	Big Data Platform	
	Infrastructure	

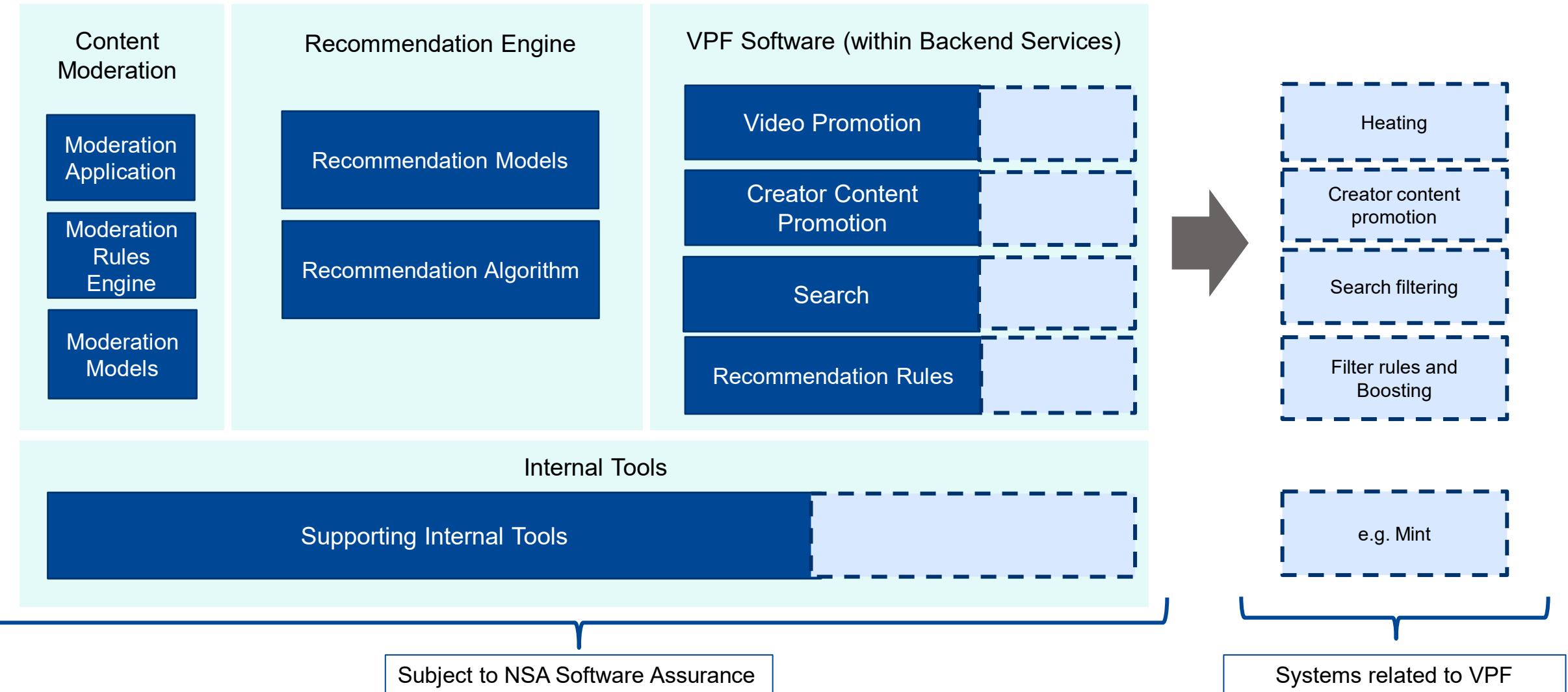*Note:* *All of the above are subject to software assurance by Oracle and the Source Code Inspector*

Current Commitments on Software Assurance

Software Review	• Dedicated Transparency Center framework underway • All code will go through the Software Assurance process • Second Source Code Inspector to augment Oracle's analysis – RFA recently issued
Software Build & Deployment	• Oracle will compile the mobile app and deliver to app stores • USDS will control the build pipeline • Software will not be permitted to run unless it goes through the Software Assurance process
Code Migration Already Underway	• All source code for gateways will transition to Oracle • All source code for access into the TTP will transition to Oracle and USDS-controlled commercial software (Global Protect VPN, Google IDP, Oracle MFA, and Oracle Gateway)

We continue to believe access to source code and rights to escalate matters of concern should define the scope of protection of U.S. national security concerns related to TikTok software and any further requirements to migrate code development to U.S. persons is inconsistent with global industry norms.

Stack View of Content Assurance Proposal

APP-382

Specific Considerations of Code Migration Proposal

Specifics of Migration Proposal	• VPF Software development migrated to Authorized Personnel • "Authorized Personnel" means only TikTok employees working in approved locations outside of China • Appropriate technical controls to ensure only Authorized Personnel work on VPF Software • Third party oversight and audit of VPF Software assurance system
Video Promotion & Filtering ("VPF") Software	• "Heating": promotions for editorial reasons based on content we believe users want to see • "Boosting": promotions to improve user growth and retention • "Creator Content Promotion": Individual users can promote a video for a fee to attract more views or followers • "Filtering": removal of content in violation of Community Guidelines
Proposed Timeline	• 6 months – 1 year • Contingent on agreed Authorized Personnel scope • Contingent on availability of internal reference code from global development

APP-383

Additional Considerations Related to Timing

1	Need to further expand development workforce outside of China to be able to operationalize code migration proposal.
2	Need to have flexibility to hire developers who meet local immigration requirements in countries beyond the U.S. such as Australia and Canada consistent with global industry standard hiring practices. Notably, many U.S. based tech companies, including direct competitors rely on a global work force, including Chinese engineering talent.
3	Need to be able to use existing tools and processes for development, build, and testing of software.
4	ByteDance software will continue to be available as a reference library for non-China teams to be used at their discretion.

APP-384

Exhibit M

NATIONAL SECURITY AGREEMENT CFIUS CASE 20-100

Presentation to the Committee on Foreign Investment in the United States

September 8, 2023

ByteDance Participants

- **Erich Andersen** – General Counsel
- **Will Farrell** – Interim lead of Security for TikTok USDS
- **Ted Gizewski** – Head of Legal & Compliance, USDS
- **Sarah Aleem –** Chief of Staff, USDS

Counsel

- **Michael Leiter** (Skadden), **David Fagan** (Covington), **Brian Williams** (Covington), **Tatiana Sullivan** (Skadden), **Katie Clarke** (Skadden), and **Monty Roberson** (Covington) on behalf of ByteDance

Topics for Today's Discussion

1	Update on Recent Milestones
2	Content Assurance Overview
3	Governance Alignment
4	Source Code Migration
5	Rethinking Source Code Inspector Function
6	Next Steps

Recent Milestones
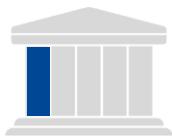
USDS Growth

- Moved employee contracts & payroll into TikTok USDS Inc.
  - FTE Count: 1,730 (as of August 25, 2023)
  - 2023 Year end FTE projection: ~2,200

Data Storage & Access

- Data deletion began in March 2023
- Gateways are operational and being tested by Oracle

Software Assurance

- Oracle now has access to 100% of source code, including recommendation engine
- Mobile sandbox is in testing & deployed to a small number of TikTok users

Content Assurance

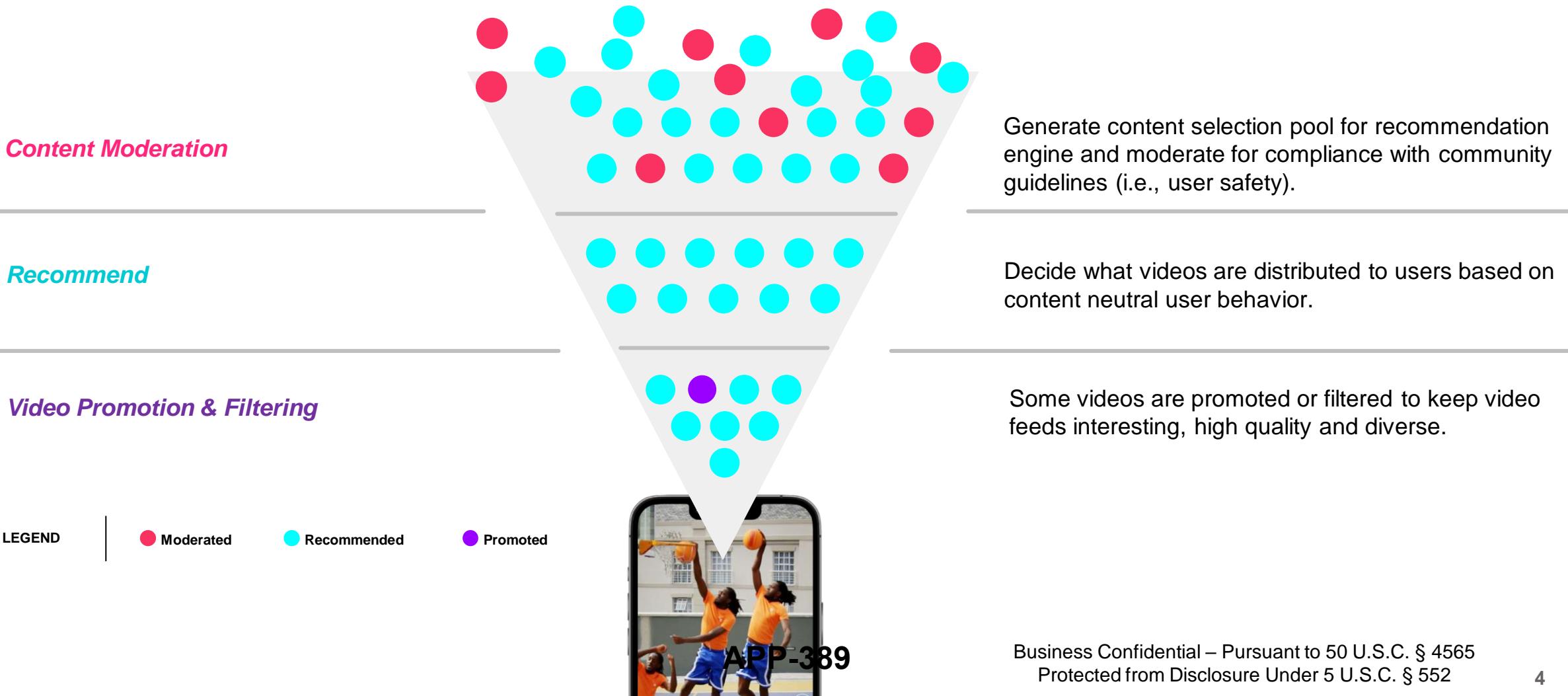- TikTok platform source code review started by Oracle
- Over 100 academic institutions have applied for access to research API; most are being approved by the company

Third-Party Oversight

- RFPs for third-party oversight roles ready to issue; pending further clarification (see slide 17)
- Data deletion auditor selected and in place
- We continue to inform and educate prospective USDS Board of Director candidates

An Overview of Systems That Determine What Users See

Content Moderation

Generate content selection pool for recommendation engine and moderate for compliance with community guidelines (i.e., user safety).

Recommend

Decide what videos are distributed to users based on content neutral user behavior.

Video Promotion & Filtering

Some videos are promoted or filtered to keep video feeds interesting, high quality and diverse.

LEGEND | ● Moderated   ● Recommended   ● Promoted

APP-389

4

Video Promotion & Filtering: Overview

TikTok promotion platforms are designed to increase user visibility to and engagement with content. **Business rules** are deve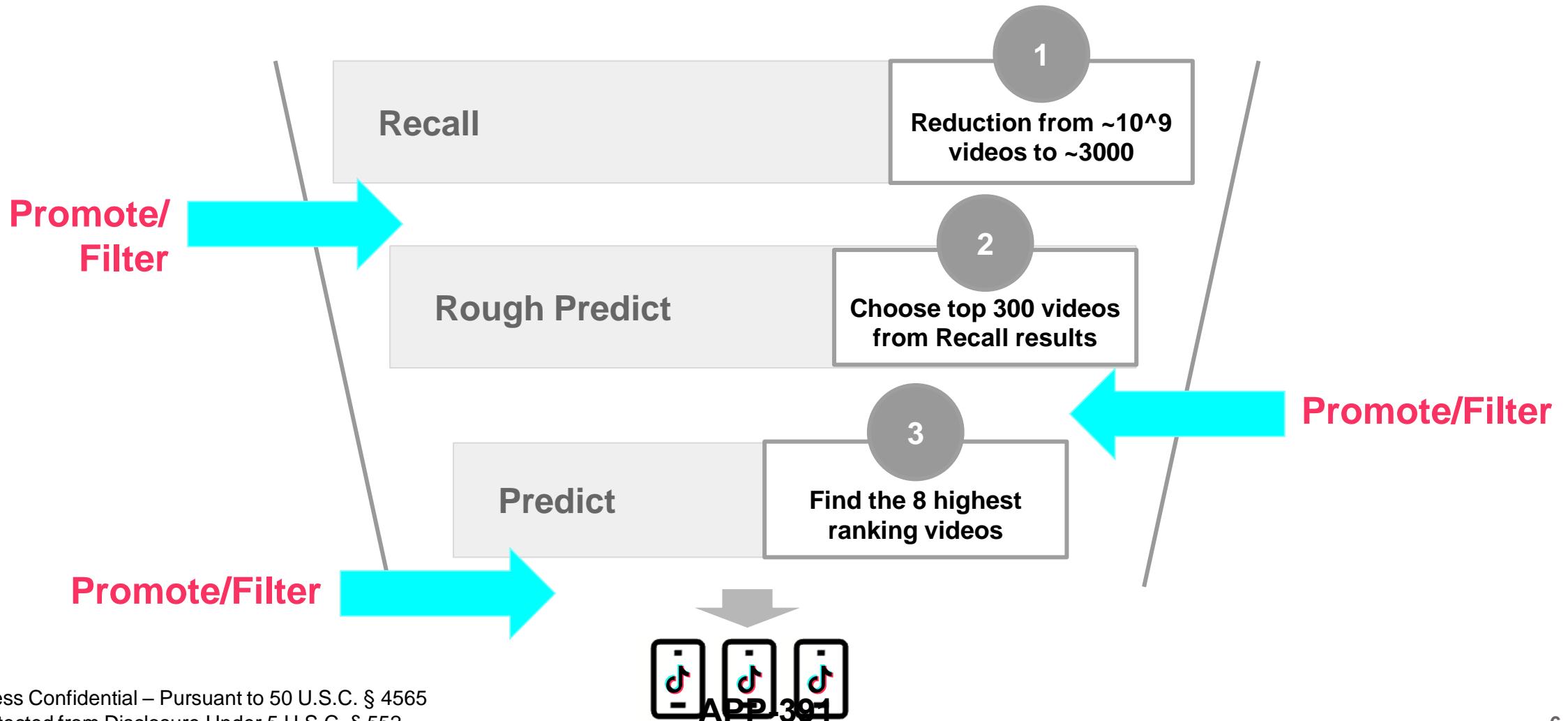loped in accordance with internal business goals to both promote and filter videos categorically (e.g., promote high-quality and local videos; decrease recommendation of identical videos).

Promotion

Heating
Promoted content is designed to provide a **diverse** TikTok experience and **support creators.** The selection process for promoted videos must align with **TikTok Editorial Guidelines**.

Boosting
Application of **rules** to the **recommendation engine** to improve user experience (e.g., new user growth).

Filtering

Filtering is used to **keep content engaging** through decreasing visibility of low-quality videos, sharing new content, and de-duplicating content.

Video Promotion & Filtering: Business Rules

Business rules are applied to the recommendation engine to serve internally defined business goals. These rules can either **boost** (promote) or **filter** content, depending on the goal TikTok is trying to achieve.

Promote/ Filter

Recall

1

Reduction from ~10^9 videos to ~3000

Rough Predict

2

Choose top 300 videos from Recall results

Promote/Filter

Predict

3

Find the 8 highest ranking videos
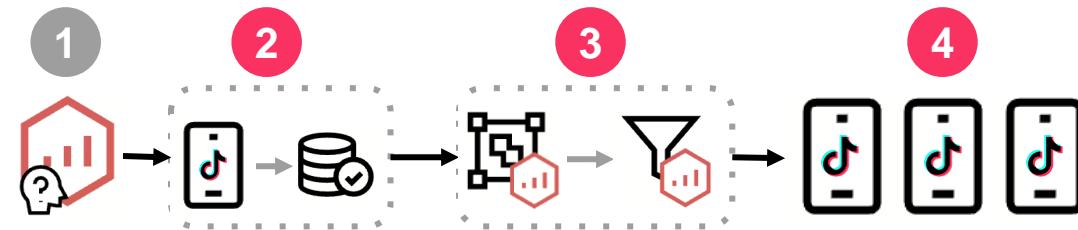
Promote/Filter

APP 391

Video Promotion & Filtering: Process Flow

The drivers for content promotion and filtering come from internal business goals. Depending on the goal, it is desirable for the visibility and engagement of content to increase (**promotion**) or decrease (**filtering**).

TikTok Promotion Platforms (heating)

1	Internal content teams select videos for promotion (e.g., content partnerships to promote individual videos)
2	Program ID created for promotion; content is promoted via promotion platform
3	Content associated with the Program ID is promoted
4	Promotion can result in increased views or engagement with content

Business Rules (filtering and boosting)

|	
1	Internal business goals set (e.g., reduce ANSA, filter extremely long videos, promote high-quality videos)
2	Business rules are developed and applied to recommendation system
3	Recommended content is refined in accordance with internal business goals

APP-392
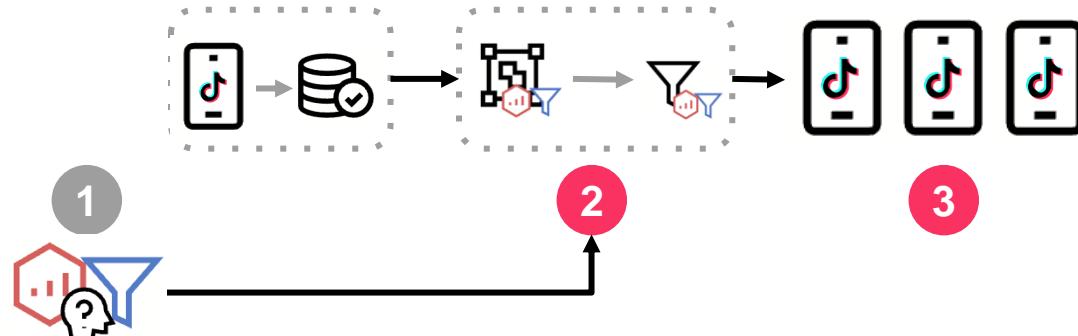
Video Promotion & Filtering: Assurance Flow

All individual videos to be promoted must be associated with a USDS-approved Program ID. Similarly, USDS approval is required to promote or filter videos categorically via new or changed business rules.

TikTok Promotion Platforms

2.1	USDS review and approval required for Program ID creation for promotions targeting the US
2.2	Promotion activities (e.g., push notifications, inbox notifications) must be linked to an approved Program ID
2.3	USDS personnel selectively audit promotion activities
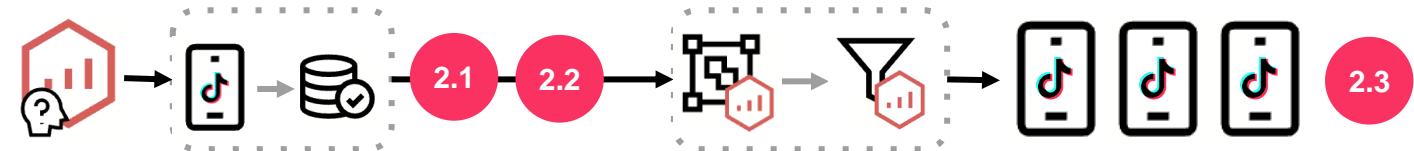
Business Rules

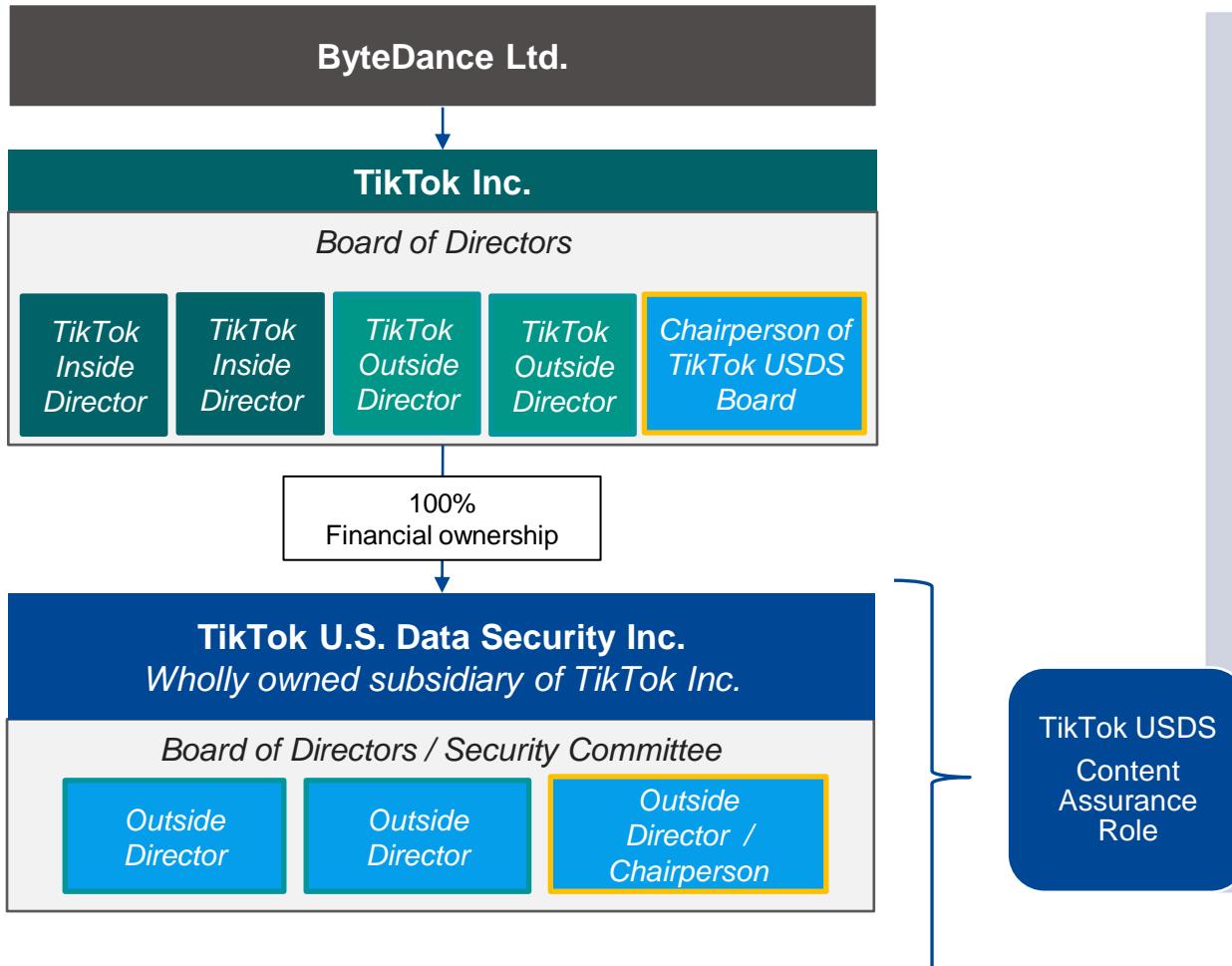|	
1.1	All rules published in the **TikTok Content Strategy Platform (TCSP)** for transparency
1.2	USDS approval required for new or changing business rules
1.3	Automatic reporting of changed rules via TCSP
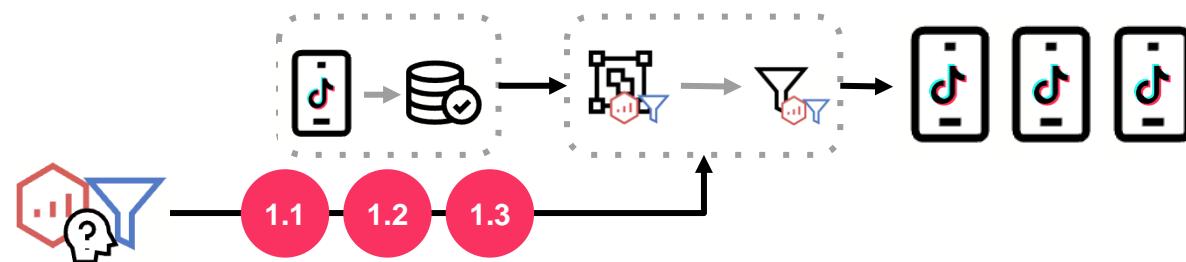
Our Trusted Technology Provider, Oracle, assures the software implementation of our promotion and filtering mechanisms.

APP-393

Overview of Global TikTok Content Assurance System
in Development
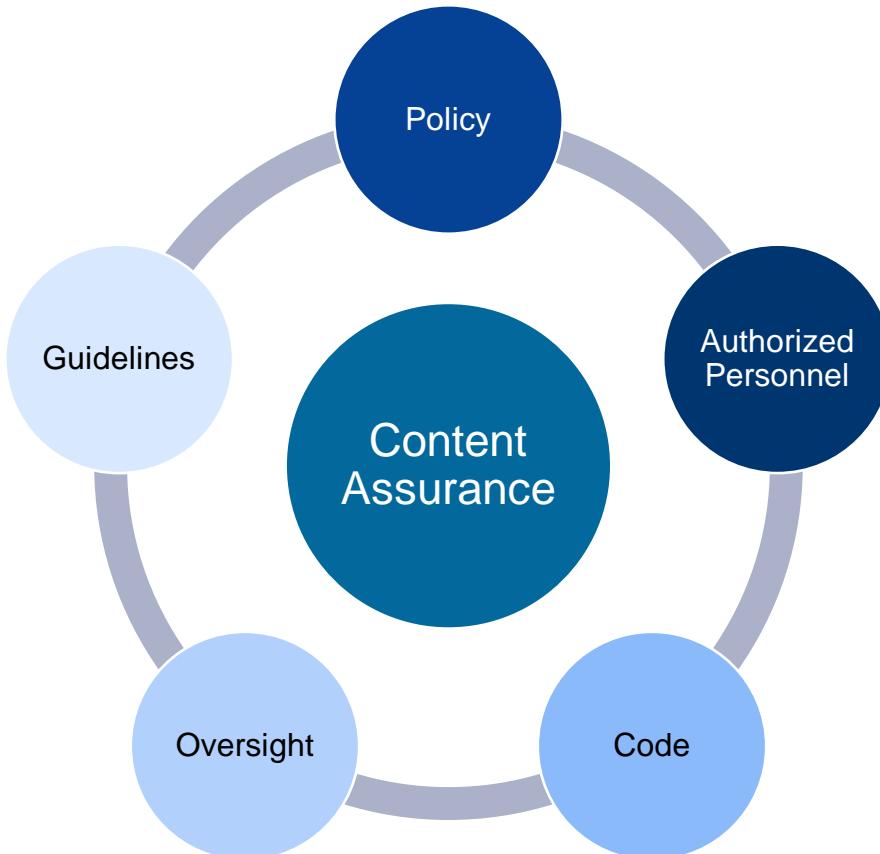
- **Policy:** Policy will prohibit any TikTok employee or contractor from taking steps to advance the political interest or agenda of any state actor with respect to TikTok content. ***Any violations of the Policy will result in disciplinary action up to and including termination.***

- **Guidelines**: Boosting, heating and filtering content will be performed only within the scope of written guidelines developed by authorized personnel in locations where TikTok is available; the guidelines will be transparent to internal teams and reviewable by third parties, such as our global content advisory committees.

- **Authorized Personnel:** Only authorized personnel will design, develop, and update content guidelines and code that implements heating, boosting and filtering of TikTok content.

- **Code:** TikTok source code in the U.S. is reviewable by Oracle under the NSA governance framework. Company has launched a research API and has already granted access to 47 independent academic institutions including Harvard, Florida Atlantic, and the University of Minnesota.

- **Oversight:** All controls related to content assurance system will be made available for inspection and monitoring by independent third parties. TikTok also is subject to DSA VLOP requirements in Europe.

APP-394

Relationship to USDS Governance Framework

ByteDance Ltd.

TikTok Inc.

Board of Directors

| TikTok Inside Director | TikTok Inside Director | TikTok Outside Director | TikTok Outside Director | Chairperson of TikTok USDS Board |

100% Financial ownership

TikTok U.S. Data Security Inc.
Wholly owned subsidiary of TikTok Inc.

Board of Directors / Security Committee

| Outside Director | Outside Director | Outside Director / Chairperson |

TikTok USDS Content Assurance Role

- **Policy & Guidelines**
  - USDS will have specific approval rights as it relates to approval and execution of guidelines.

- **Authorized Personnel**
  - Limited list of pre-authorized USDS personnel who are permitted to approve guidelines.
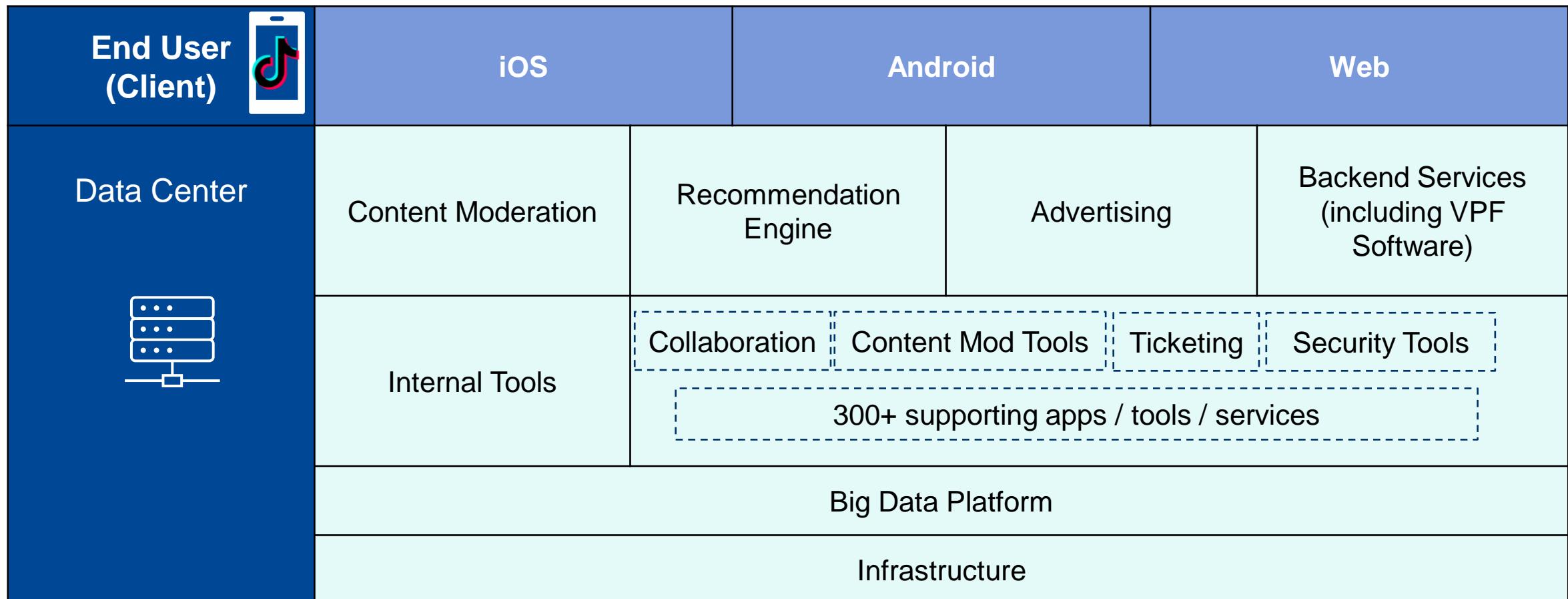
- **Code**
  - All code will go through Oracle's software assurance process prior to deployment.
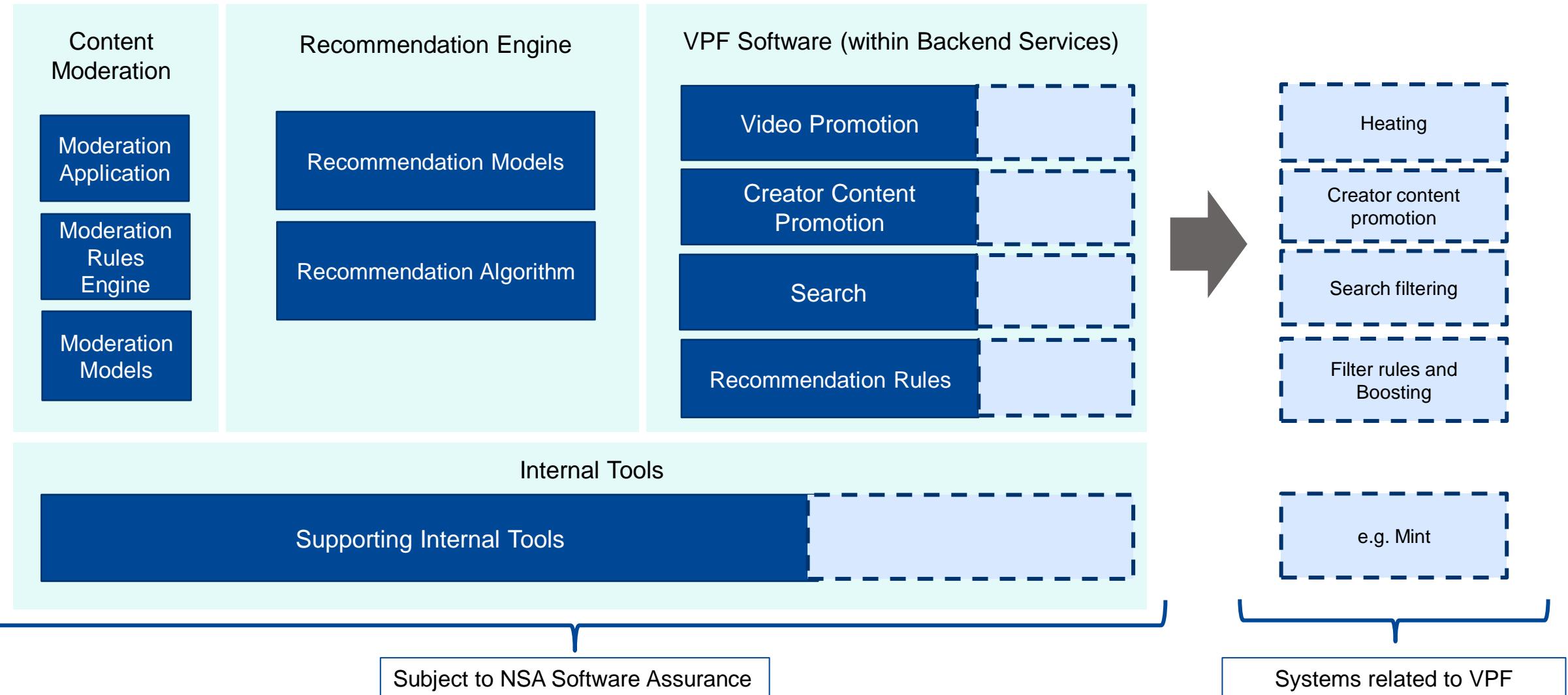 - Content Assurance code will be deployed by USDS.

- **Oversight**
  - Several layers of oversight, including Oracle, Content Advisory Council, Third Party Monitor, and Third Party Auditor.

APP-395

High Level Stack View of TikTok Systems

End User (Client)	iOS	Android		Web
Data Center	Content Moderation	Recommendation Engine	Advertising	Backend Services (including VPF Software)
	Internal Tools	Collaboration · Content Mod Tools · Ticketing · Security Tools		
		300+ supporting apps / tools / services		
	Big Data Platform			
	Infrastructure			

Note: *All of the above are subject to software assurance by Oracle and the Source Code Inspector*
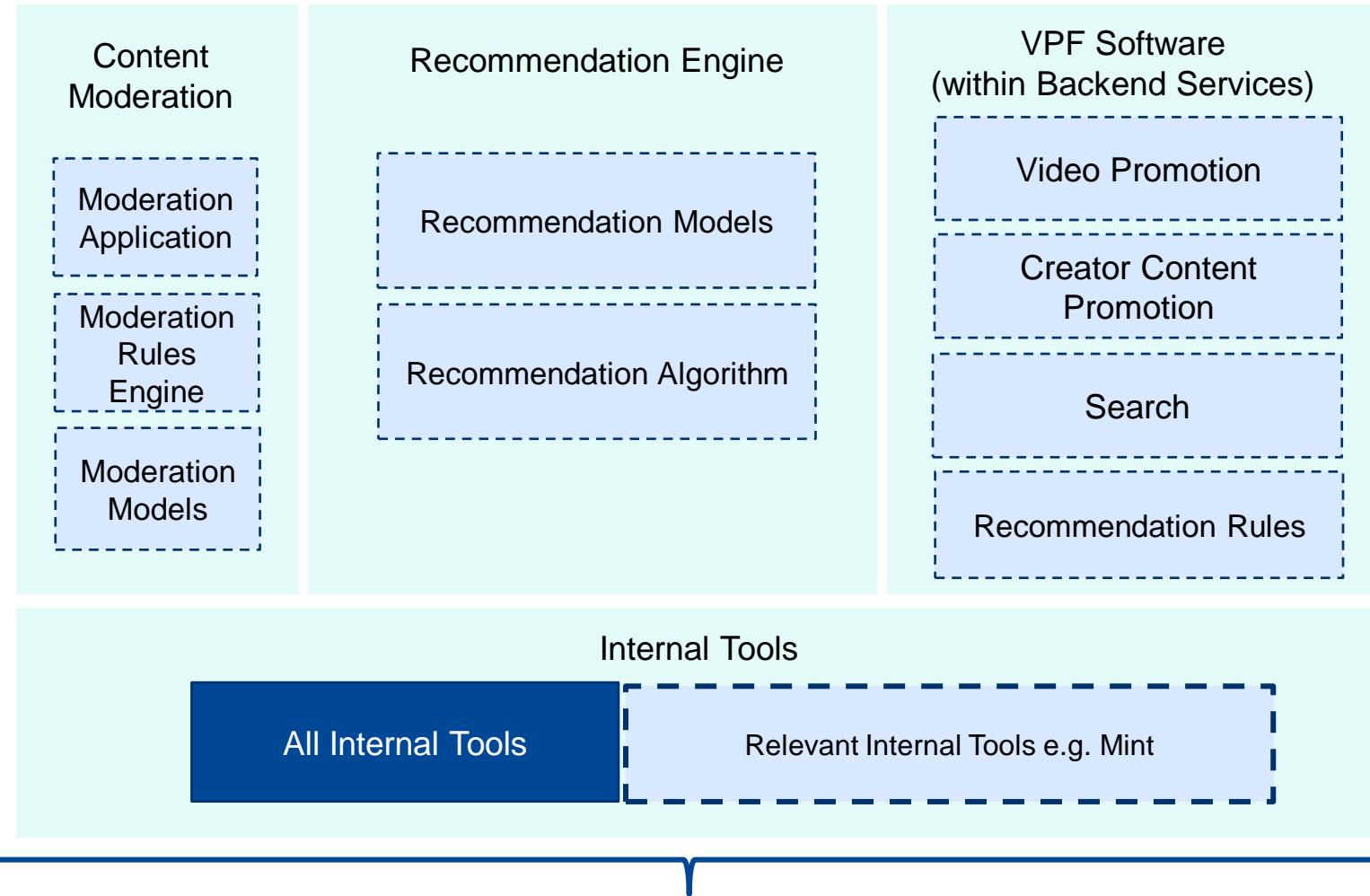
Stack View of Software Migration Proposal

Specific Considerations of Software Migration Proposal

Global Development Considerations and Controls	• VPF Software development migrated to Authorized Personnel • "Authorized Personnel" means only TikTok employees working in locations where the TikTok service is offered • Appropriate technical controls to ensure only Authorized Personnel work on VPF Software • Third party oversight and audit of VPF Software assurance system
Proposed Timeline	• Approximately 6 months – 1 year from agreement • Contingent on agreed Authorized Personnel scope • Contingent on availability of internal reference code from global development

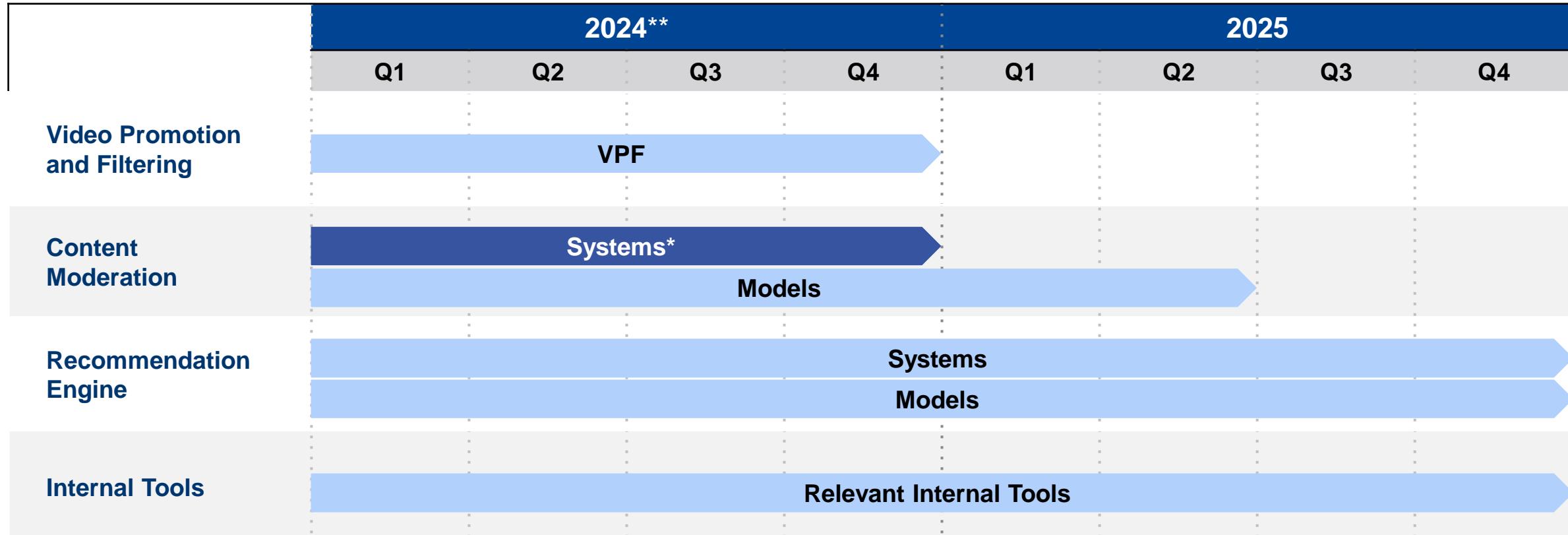**APP-398**

Stack View of Software Migration Alternative

Response to May 2023 meeting request

Content Moderation	Recommendation Engine	VPF Software (within Backend Services)
Moderation Application	Recommendation Models	Video Promotion
Moderation Rules Engine	Recommendation Algorithm	Creator Content Promotion
Moderation Models		Search
		Recommendation Rules

Internal Tools

All Internal Tools	Relevant Internal Tools e.g. Mint

Subject to NSA Software Assurance
APP-399

Specific Considerations of Alternative

Company's View	• Not recommended - anticipate complexity in managing risk of incompatible systems with independent development of alternative recommendation engine • Code migration at broader scale is unnecessary, given full set of protections: content assurance system + full access to source code by highly qualified third parties = comprehensive solution • Anticipate significant challenges in hiring qualified engineers to pursue independent development • Cost for company in competitive and dynamic market is very high
Specifics of Migration Proposal	• "Authorized Personnel" means only TikTok employees working in locations where the service is commercially available • Need access to global internal reference code or ability to release via open source • Appropriate technical controls to ensure only Authorized Personnel work on software in scope • Third party oversight and audit

Estimated Software Migration Timeline

	2024**				2025			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

Software

Video Promotion and Filtering
VPF

Content Moderation
Systems*
Models

Recommendation Engine
Systems
Models

Internal Tools
Relevant Internal Tools

*Content Moderation Systems will continue to be developed in China but be subject to open source to the public.
**Start Date: 1/1/2024 with an assumption of a signed NSA

APP-401

Rethinking Source Code Inspector Function

Current NSA Scope		Proposed Change
• "Source Code Inspector" is defined in 9.11		• Rename to "Independent Security Inspector"

• Scope:
    • An independent inspector of Source Code and Related Files in the DTC
    • Conduct Source Code security vulnerability assessments within DTCs
		• Broader Scope:
		    • Independent security risk and vulnerability inspector of TikTok U.S. Platform
		    • Perform security testing necessary to identify gaps and flaws in TikTok's software and systems
		    • RFP vendors with experience on combatting nation state adversaries

• Submit reports directly to CMAs and Third-Party Monitor on CMA determined schedule		• Submit reports directly to CMAs and Third-Party Monitor on CMA determined schedule
• Submit quarterly reports to Transaction Parties, TTP, and Third-Party Monitor		• Submit quarterly reports to Transaction Parties, TTP, and Third-Party Monitor

APP-402

Conclusion and Next Steps

APP-403

Appendix

APP-404

Content Moderation

APP-405

Content Moderation: Overview

Content Moderation is a combination of specialized technology (auto-moderation) and human moderators who are trained to recognize violative content and make policy decisions accordingly. This process generates the content pool for the recommendation engine.
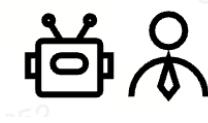
Enforces Community Guidelines	Advised by Content Advisory Council (CAC)	Composed of both automated and human moderation
The TikTok **Community Guidelines** are a publicly available code of conduct to ensure user safety and a friendly digital environment. A violation of the guidelines may result in the account and/or content being removed.	The **TikTok Content Advisory Council** advises the business on a variety of topics, including child safety, hate speech, misinformation, and bullying, with members hailing from the technology, policy, and heath and wellness industries.	TikTok has combined content moderation technology with a robust human moderation team and several layers of tools and processes to recommend **safe** content to users.

Content Moderation: Routes to Moderation

There are three avenues through which content is included in automated and human moderation queues. ~400 million videos are published each month; on average, 3% of all published videos underwent human moderation.

First Publish

- Auto-moderation is trained on text, video, image, and behavioral signals to identify violative content
- If auto-moderation has low confidence in its decision (whether to publish, to not recommend, or to take down content), the content is passed to human moderators to review

Viral Content

- If content has exceeded certain viewership thresholds, it is recalled to human moderators for review

User Reporting

- Users can report any videos through the TikTok app
- Reported videos are automatically flagged for review by human moderators

Content Moderation: Process Flow

While our AI conducts auto-moderation activities, human moderation teams may also review content per the process articulated below. Human moderation may include multiple rounds of review.

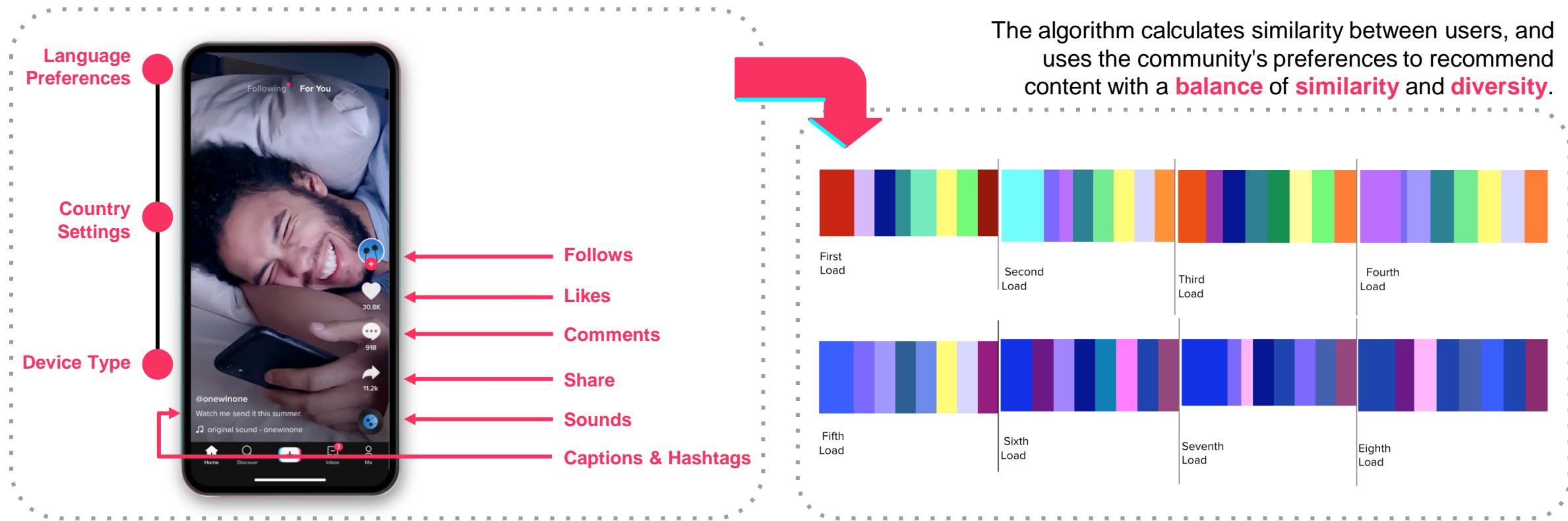|	
1	User **uploads** content
2	Auto-moderator reviews content and makes a **decision**
3	If the auto-moderator has low **confidence**, human moderators review and if needed enforce on content
4	If content is **approved**, it is published
5	After publication, content can go **viral** or be reported by **other users**
6	Human moderators review and, if needed, enforce on flagged content

APP-408

Recommendation

APP-409
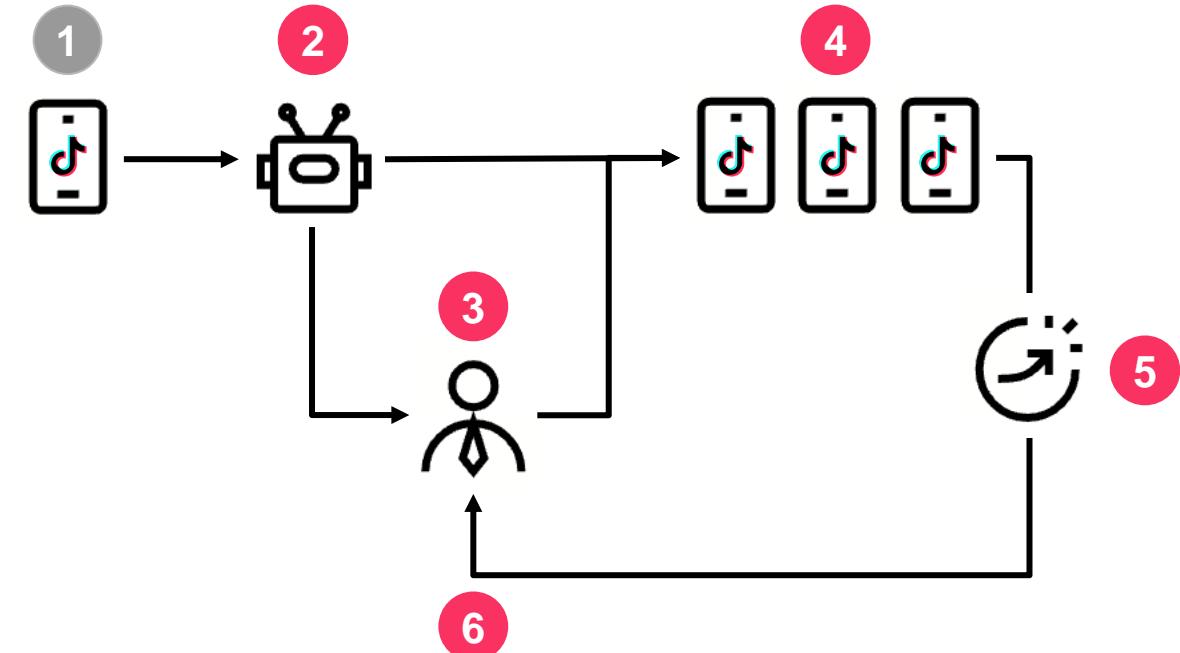
Recommendation: Overview

The recommendation engine is a complex set of models designed to provide **tailored content** and instantly respond to **users' preference at the moment** when they interact with app. This content is selected by a complex calculation of **users' behaviors** optimizing for **maximizing the value of users / creators and the platform**.

The algorithm calculates similarity between users, and uses the community's preferences to recommend content with a **balance** of **similarity** and **diversity**.

Language Preferences

Country Settings

Device Type

Follows

Likes

Comments

Share

Sounds

Captions & Hashtags

First Load

Second Load

Third Load

Fourth Load

Fifth Load

Sixth Load

Seventh Load

Eighth Load

APP-410

Recommendation: Process Flow

Multiple rounds of video ranking and shuffling are designed to optimize a batch of 8 videos, algorithmically selected from a content pool of millions of videos, to present to a single user.

|	
1	User **uploads** content
2	Content moderation completed; approved videos move to **content pool**
3	Recommendation engine **predicts** the likelihood a user will engage with the videos in the content pool
4	Recommendation engine **ranks** videos by combining different engagement likelihood
5	Top 8 recommended videos are shared in **For-You Feed**
6	User implicit and explicit **feedback** is used to improve quality of recommendations
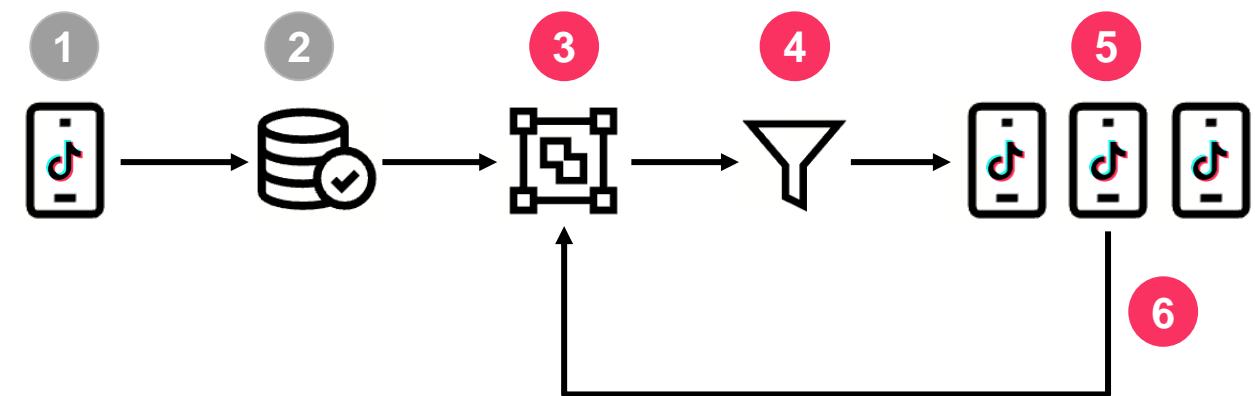
Exhibit N

Redacted Version

April 1, 2024

David Newman
Principal Deputy Assistant Attorney General for National Security
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Mr. Newman:

We write on behalf of our client ByteDance Ltd. (together with relevant subsidiaries, "ByteDance" or the "Company") in response to your emails dated March 14 and 18, 2024, with reference to Case No. 20-100 before the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"). To confirm, in response to your March 14 email, we are prepared to meet with you and Assistant Secretary of the Treasury Paul Rosen in early April to continue— or more accurately, restart, given the U.S. government's extended hiatus from speaking with the Company—discussions of solutions that can be implemented and fully address U.S. national security interests. Before we have that meeting, however, we feel it is important to address several points raised in your correspondence.

We reiterate that ByteDance remains committed to resolving this matter through a negotiated agreement with the Committee. This has been the Company's steadfast position over the course of the four and a half years that the matter has been pending before CFIUS. And, as you know, it is the *exact* position that the Company expressed in your meetings with the Company last year. At all times, the Company has approached the CFIUS process with respect. It has been responsive, transparent, and constructive as it has worked toward finding solutions and advancing the U.S. government's publicly-stated objectives: to ensure the safety of TikTok's U.S. users and the integrity of the TikTok U.S. platform, including against misinformation campaigns. The Company has approached this process responsibly and constructively in the face of the *ultra vires* exercise of authority by the U.S. government, an extraordinary public campaign against it, increasingly led by the very officials in the U.S. government with statutory responsibility for the CFIUS process, and against a history with CFIUS preceding the August 14, 2020 Executive Order that was violative of the law and offensive to the most basic notions of fairness and due process.

The Company had substantial hope that normalcy and a respect for CFIUS and the law that governs it would return in January 2021. And indeed, from January 2021 through August 2022, the Company and the Committee worked constructively through an intensive fact-based process to build a solution that could be codified in an agreement and resolve any dispute over the August 14, 2020 Executive Order. We explained in those discussions, as well as in earlier submissions, presentations, and meetings leading into January 2021, that ByteDance formed and grew the technology underlying the TikTok platform organically. As a result, and as the Company made clear in discussions and various submissions, ByteDance could not divest the TikTok U.S. platform because: TikTok did not acquire the underlying technology for the platform (*i.e.*, its

APP-413

algorithm), but rather it was developed internally by ByteDance; the technology was been developed in China and was (and remains) subject to Chinese export control laws; and the Chinese government had asserted that those laws forbid any negotiated agreement with CFIUS that would require a divestiture of the TikTok algorithm.

Over the course of 2021, the Company provided additional detailed presentations and submissions to CFIUS regarding the operations, processes, and governance and management of the TikTok U.S. platform, including on the key issues of importance to the U.S. government—including the collection, access to, and safeguarding of U.S. user data; software development, deployment, and security validation of the TikTok source code; and assurance processes related to content, which covered the trust and safety operations and how the platform and processes operated to address potential malign foreign influence. Through these presentations and submissions, the record before CFIUS made clear that (1) there was not a practical way to divest TikTok's U.S. operations; (2) the Chinese government had stated that it would block any such divestiture; and (3) any effort to isolate the U.S. platform would be subject to continuing dependencies on ByteDance and the rest of the global TikTok business. On the basis of these presentations and submissions, the Company and CFIUS worked to develop a detailed 90-page National Security Agreement ("NSA") that, in painstaking detail, addressed each of the concerns raised by CFIUS, culminating in a draft NSA transmitted to CFIUS on August 23, 2022 (Exhibit A).

In parallel, as has been documented, the Company began voluntarily implementing the solution, including moving protected U.S. user data and the TikTok U.S. platform to the cloud environment of the Trusted Technology Provider (*i.e.*, Oracle); providing control over such data and systems to TikTok U.S. Data Security, managed by U.S. persons; and establishing a Dedicated Transparency Center to enable security inspections, reviews, and verification of TikTok Source Code and Related Files. To date, the Company has spent more than $2 billion on this solution.

The hallmarks of the solution reflected in the August 23, 2022 draft NSA—the implementation of which are underway—include:

- **No data access from China**. All protected U.S. user data—including expatriate data—will be safeguarded in the United States under a special corporate structure (TikTok U.S. Data Security) and the protections of the Trusted Technology Provider (Oracle). [NSA Articles 2, 3, 8, and 11.]

- **All software code—app and backend—secured by a U.S.-based and U.S. government-approved Trusted Technology Provider (*i.e.*, Oracle)**. The TikTok U.S. platform and TikTok U.S. app will be deployed through Oracle infrastructure and subject to source code review/vetting by Oracle with another CFIUS-approved third party responsible for conducting security inspections. [NSA § 8.4 and Article 9.]

- **Content moderation transparency and compliance**. The draft NSA includes multiple layers of protection to address concerns related to content available on the platform, including ensuring that all content moderation—both human and algorithmic—is subject to third-party verification and monitoring. [NSA §§ 5.4, 9.13, 16.6.]

- **Separation of the business responsible for the foregoing from China**. The draft NSA requires a special board, with Security Directors whose appointment would be subject to the U.S. government's approval and would exclude ByteDance and its subsidiaries and affiliates, to oversee TikTok U.S. Data Security. [NSA § 3.1.] In addition, further separation between ByteDance and its subsidiaries and affiliates, including TikTok in the rest of the world, and U.S. operations would be achieved by appointing a U.S. government-approved Security Director to the board of TikTok Inc., TikTok U.S. Data Security's immediate parent. [NSA § 4.1.] As you know, the Company recruited distinguished potential directors with extensive national security experience and shared their names and backgrounds with CFIUS.

- **Unprecedented layers of review, monitoring, and auditing**. The draft NSA includes multiple layers of monitoring and auditing, which include not just the Security Directors responsible for the TikTok U.S. Data Security governance structure (with a Security Director also on the board of TikTok Inc.), but also the Trusted Technology Provider (Oracle); the Content Advisory Council; a third-party monitor; third-party auditor; third-party security inspection of source code; and the CFIUS monitoring agencies themselves. [NSA §§ 5.4, 8.1, 8.2, 9.11, 14.1, 15.1, 16.1, 17.1, 17.2.]

- **Strict penalties for noncompliance**. These penalties include a "kill switch" (which would give CFIUS the explicit authority to suspend the platform in the United States at the U.S. government's sole discretion in response to specified acts of noncompliance) and significant monetary penalties. [NSA §§ 21.3-5.]

Throughout this process, it was also repeatedly made clear to CFIUS that ByteDance was majority-owned by global investors, including substantial U.S. investors; that TikTok was implementing data security protections beyond any other peer in industry; and that TikTok is a globally interoperable and integrated platform, such that separating the U.S. platform would, as a matter of fact, be impossible and akin to a peer company trying to divest the U.S. part of a global social media platform.

Nevertheless, after our submission of the draft NSA on August 23, 2022, the Committee —for reasons that have never been explained despite numerous entreaties from counsel—ceased any substantive negotiations. At the same time, senior officials in the U.S. government began speaking publicly against the Company, undermining the confidential process that led to significant progress over the prior year and a half.[1] From August 2022 through March 2023, the

---

[1] Lauren Hirsch, David McCabe, Katie Benner and Glenn Thrush, "TikTok Seen Moving Towards U.S. Security Deal, but Hurdles Remain," New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html ("The Justice Department is leading the negotiations with TikTok, and its No. 2 official, Lisa Monaco, has concerns that the terms are not tough enough on China, two people with knowledge of the matter said."); Eric Tucker, "FBI director raises national security concerns about TikTok," AP News (Dec. 2, 2022), https://apnews.com/article/technology-china-united-states-national-

(cont'd)

APP-415

Company responded to certain limited information requests from CFIUS, and proactively provided updates to CFIUS, but CFIUS declined to engage in any additional negotiations about the draft NSA. CFIUS rejected or ignored multiple requests from the Company to meet with CFIUS staff and the "Deputies" (the Deputy Secretary-level officials of the CFIUS member agencies who ultimately oversee the Committee); did not respond to an offer from the Company to visit and inspect its Dedicated Transparency Center in Maryland; and refused the Company's request to include other member agencies of the Committee in meetings and discussions with the Company. Again, these requests for engagement occurred during the *exact* period that the Administration officials responsible for CFIUS continued to comment on the issues publicly.

This brings us to your emails from March 14 and 18, 2024. What seems clear from those emails—and the reported efforts of the Department of Justice ("DOJ") to support legislation that would effectively ban TikTok in the United States[2]—is that this Administration has determined that it prefers to try to shut down TikTok in the United States and eliminate a platform of speech

---

security-government-and-politics-ac5c29cafaa1fc6bee990ed7e1fe5afc ("Wray said the FBI was concerned that the Chinese had the ability to control the app's recommendation algorithm, 'which allows them to manipulate content, and if they want to, to use it for influence operations.'"); "Treasury Secretary Janet Yellen on TikTok national security fears," 60 Minutes (Dec. 9, 2022), *available at* https://www.youtube.com/watch?v=rdSjccn29F0 ("They have access to a lot of data on your teenager from the information they collect while your teenager is online."); Gavin Bade, "TikTok national security deal roiled by internal strife," Politico (Dec. 16, 2022), https://www.politico.com/news/2022/12/16/biden-administration-at-odds-over-forcing-tiktok-divestment-00074415 ("The Biden administration is at odds over whether to force the Chinese owner of TikTok to divest from its U.S. operations, according to five people with knowledge of the discussions . . . ."); Stu Wu, Kate O'Keefe, and Aruna Viswanatha, "TikTok Security Dilemma Revives Push for U.S. Control," Wall Street Journal (Dec. 26, 2022), https://www.wsj.com/articles/tiktok-security-dilemma-revives-push-for-u-s-control-11672064033 ("'We're talking about a government that, in our own intelligence community's estimation, has a purpose to move global technology use and norms to privilege its own interests and its values, which are not consistent with our own,' Deputy Attorney General Lisa Monaco said in an interview, in which she declined to discuss TikTok specifically."); Hannah Rabinowitz, "US deputy attorney general: 'I don't use TikTok, and I would not advise anyone to do so,'" CNN (Feb. 16, 2023), https://www.cnn.com/2023/02/16/politics/tiktok-monaco-us-disruptive-technology-strike-force/index.html.

[2] Natalie Andrews et al., "TikTok Crackdown Shifts Into Overdrive, With Sale or Shutdown on Table," Wall Street Journal (Mar. 10, 2024), https://www.wsj.com/tech/why-the-new-effort-to-ban-tiktok-caught-fire-with-lawmakers-7cd3f980 ("Key to smoothing out this effort was Deputy Attorney General Lisa Monaco, people familiar with the matter said. . . . Monaco helped draft the legislation, and her presence as a Biden administration senior official helped congressional Democrats buy into supporting the bill, one of the people said."); Chris Strohm, Daniel Flatley, and Alex Barinka, "DOJ to Push for TikTok Divestiture in Senate Briefings," Bloomberg (Mar. 18, 2024), https://www.bloomberg.com/news/articles/2024-03-18/biden-officials-to-brief-wary-senators-on-tiktok-sale-push.

for 170 million Americans, rather than continue to work on a practical, feasible, and effective solution to protect U.S. users through an enforceable agreement with the U.S. government. It also now appears that the Company's engagement with CFIUS in good faith in a confidential process was leveraged by DOJ for purposes of crafting that legislation. To be clear, if the legislative approach being advocated by DOJ (which is the same approach articulated by CFIUS in March 2023) survives judicial review, the reality—which you know well based on the Company's engagement with DOJ and the Department of the Treasury since March 2023—is that there will be no sale of TikTok, qualified or otherwise, and the TikTok platform will cease to exist in the United States.

With the foregoing as background, we turn more specifically to responding to your emails from March 14 and March 18:

> **A. Your email from March 14 states:** *"As you know from our discussions over the past year, senior officials across the U.S. government have thus far identified only one viable solution to resolve the USG's national security concerns related to TikTok: An orderly divestment by ByteDance of the assets (including source code and algorithms) used to enable TikTok's U.S. operations in tandem with an assurance that ByteDance does not have continued ownership over TikTok's U.S. operations and that TikTok U.S. user data is not accessible to ByteDance or the Chinese government."*

As noted above, while your email refers to "discussions over the past year," there have been no discussions over the last year between the Company and "senior officials across the U.S. government," nor was there any engagement with the Company *at all* between September 2022 and March 2023 on a negotiated resolution of the Government's national security concerns. Even when the government finally informed the Company of its divestiture position in March 2023, it provided a wholly conclusory statement to the Company about how "senior officials" arrived at this position, and never explained why the U.S. government believes that its purported "solution" is actually feasible. To the contrary, the record before CFIUS makes clear that the government's divestiture position is commercially and technologically ***not viable***, particularly under the timeframes dictated by the government.

As you know, the government's position regarding divestment (including source code and algorithms) to which your March 14, 2024 email refers was first provided to the Company's outside counsel on March 6, 2023, in a call arranged by Assistant Secretary Rosen after seven months of non-engagement. You also attended the call, along with other staff from the Department of the Treasury. During the March 6, 2023 call, Mr. Rosen stated that while the government appreciated the parties' engagement regarding the draft NSA and the responsiveness of the parties to the U.S. government at the staff level, "senior government officials" deemed the draft NSA submitted August 23, 2022 to be insufficient to address the government's national security concerns. Mr. Rosen further said that these senior officials continue to believe a negotiated outcome is achievable, and that a negotiated outcome would need to involve (1) an orderly divestment by ByteDance of U.S.-based assets supporting TikTok and (2) the migration of source code for the TikTok U.S. platform out of China.

APP-417

Regarding the government's contemplated "source code migration," you explained that the government would require development of all source code for or supporting TikTok U.S. operations to be moved to the United States, or to a location approved by the U.S. government. You acknowledged there could be a "migration period" for transitioning source code to approved locations but did not articulate a specific time. Mr. Rosen noted, however, that a period as long as a year would be "a hard pill for the government to swallow." With respect to the "orderly divestment" contemplated by the government, you stated that senior leadership had considered a structure involving "passivity" (*i.e.*, a passive ownership structure) of the TikTok U.S. platform by ByteDance, but concluded that the idea "was not sufficient," and therefore the government was not prepared to discuss it as an alternative.

During the March 6, 2023 call, counsel for the Company repeatedly sought clarity regarding the basic technological premises of the government's position on "source code migration," but was met with vague and inchoate responses. Counsel asked, for example, whether source code migration meant that all code for the U.S. platform would need to be (i) rewritten outside of China, or, alternatively, (ii) transferred from China and then monitored in the United States, with further development of the software only occurring outside of China. Counsel noted that the Company's implementation of the draft NSA required the inspection of that code, and asked whether the U.S. government's expectation was that, under its contemplated divestiture, all source code for the TikTok U.S. platform would need to be re-written. You stated that "the concept was north of what was in the NSA but south of a requirement to fully rewrite the code."

Counsel for the Company were also clear during the March 6, 2023 call that the government's divestiture position was not realistic. Counsel pointed out that CFIUS was already well-advised about the technological complexity of their contemplated divestiture given the timelines mandated by the draft NSA—which did *not* require a sale of the TikTok U.S. platform and was accordingly significantly less complex from an engineering perspective than the government's contemplated divestiture. Particularly against the backdrop of those earlier discussions, counsel explained that CFIUS knew full well that 12 months—let alone a shorter period—was not a realistic timeframe. Counsel noted that the government's position was to "effectively break apart the Company, which is a globally integrated platform." You responded by saying that a longer timeline for transition would require rigorous interim measures without explaining what those interim measures would be.

During the March 6, 2023 call, Mr. Rosen explicitly linked the CFIUS negotiations to political developments in Congress. Mr. Rosen said that there appeared to be broad bipartisan support to remove ByteDance ownership and concerns with data "traveling back to China" and "feeding ByteDance algorithms," and that congressional proposals included unilateral authority to remove TikTok in the United States. Nevertheless, Mr. Rosen stated that the Executive Branch continued to believe a negotiated agreement is the best path and "should be seriously considered by [the Company]." You emphasized that this negotiated solution should be preferable to a legislative one.

APP-418

The very next day, legislation was introduced by Senator Mark Warner that would have empowered the Secretary of Commerce and the President to prohibit, compel divestment of, or otherwise mitigate certain covered transactions and holdings that, in their determination, pose an undue or unacceptable risk to national security. It was widely reported that this legislation was intended to target TikTok and was drafted in close consultation with the Biden Administration, including DOJ.[3] Indeed, the Biden Administration endorsed the bill the same day it was introduced.[4]

In sum, by March 2023, the government had spent 18 months negotiating a robust solution addressing its national security concerns, including, in our view, unprecedented data and content assurance, only to abandon that effort and cease engaging with the Company on the solution for seven months, whereupon, without any explanation of why the previously negotiated solution was insufficient, it demanded divestment and source code migration. And the very next day, it publicly announced its support for legislation explicitly calculated to provide the Administration with additional authorities to compel the divestiture of TikTok or ban the platform outright.

> **B. Your March 14 email further states:** *"While I know that our teams have been in contact since our last briefing (and that you have provided information on these topics at earlier junctures), we and our buildings are – for understandable reasons – eager to receive an update on your client's willingness to complete such an orderly divestment as well as on the technical and related questions that we have discussed, including the migration of source code and algorithms."*

The implication of this statement in your March 14 email is that the Company has not been responsive in its engagement with CFIUS and, in particular, has failed to advise the government whether it is "willing" or "unwilling" to pursue the government's contemplated divestiture. This implication is false. As you have known for a year, the divestiture path articulated by the government on March 6, 2023 is not viable—period—let alone on any timeline the government appears prepared to accept. This is not a matter of our client's "willingness" or "unwillingness."

---

[3] Brendan Bordelon and Gavin Bade, "Senate, White House push new bipartisan bill that could ban TikTok," *Politico* (Mar. 7, 2023), https://www.politico.com/news/2023/03/07/senate-white-house-tiktok-ban-00085998 ("And while the RESTRICT Act isn't technically aimed just at TikTok, the Chinese-owned video app is clearly top of mind for the bill's chief sponsors . . . ."); Jeremy Diamond and Brian Fung, "The Biden administration is shifting its approach to TikTok," CNN (Mar. 8, 2023), https://www.cnn.com/2023/03/08/tech/biden-tiktok-bill/index.html ("The bill was drafted in close consultation with the White House's National Security Council as well as the Commerce, Treasury and Justice Departments" and "[t]he National Security Council and Department of Justice proposed specific changes to the text of the legislation, some of which were adopted . . . .").

[4] The White House, "Statement from National Security Advisor Jake Sullivan on the Introduction of the RESTRICT Act" (Mar. 7, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/07/statement-from-national-security-advisor-jake-sullivan-on-the-introduction-of-the-restrict-act/.

The record before CFIUS—both before March 6, 2023 and since then—makes clear that the government's contemplated divestiture cannot be effectuated in the way the government wants.

On March 15, 2023, counsel for the Company proposed an agenda to continue the discussion and seek additional details regarding the government's position. The proposed agenda made clear the challenges associated with the government's divestiture position, including by noting specifically the "timing and operational challenges to maintain globally integrated platform and export control issues."

Internal and outside counsel for the Company then met on March 23, 2023 via teleconference with senior staff for the Departments of Justice and the Treasury, including Brian Reissaus, Deputy Assistant Secretary for Investment Security from Treasury, and Devin DeBacker, Chief, Foreign Investment Review Section, from DOJ.

Counsel for the Company started the meeting by advising that ByteDance was glad to re-engage with CFIUS and still hoped to reach a negotiated solution, but the public discourse was "adrift from realistic facts and solutions." Counsel also noted that leaks about the government's position and public comments from Administration officials regarding CFIUS's position and the contemplated divestiture were problematic and damaging. Mr. Reissaus and Mr. DeBacker acknowledged the importance of confidentiality, although Mr. DeBacker noted the government views confidentiality as a "two-way street." (Notwithstanding Mr. DeBacker's statement, as you know, the CFIUS statute imposes an obligation of confidentiality on the government, with limited exceptions, but not private parties. *See* 50 U.S.C. § 4565(c).)

Mr. DeBacker added that the government still believed a negotiated solution could be accomplished. He then asked if ByteDance had a proposal for orderly divestiture. Counsel explained that the Company could not put a proposal on the table because it did not understand what the government meant by "divestment." Counsel explained that ByteDance needed to reconcile the government's position with three key realities:

1. how to divest the TikTok U.S. platform without turning the U.S. TikTok experience into an "island" with no interoperability with the rest of the platform, which would break the TikTok experience in the United States (as CFIUS knew, this concern had been central to multiple presentations to CFIUS over the course of 2020 and 2021);

2. the Chinese government's opposition (as CFIUS well understood, TikTok's recommendation algorithm was subject to Chinese export control laws, and the Chinese government had publicly indicated it would block the transfer, use, or licensing of the algorithm by any successor if there was a forced divestiture); and

3. "the people and code"—*i.e.*, the fact that (i) part of the technical workforce supporting the TikTok platform is located in China (similar to many U.S. headquartered peer companies with technical personnel located in China), and (ii) personnel working on tasks such as sales, marketing, and creator relations are globally integrated to support

APP-420

customers who have global (*i.e.*, not limited to U.S.) demands (again, akin to peer companies).

Counsel noted the government's months-long delay in responding prior to March 6, and observed that there had been no explanation as to why the government believed the August 23, 2022 draft NSA was deficient from a national security perspective. Counsel noted that the security personnel within TikTok U.S. Data Security and Oracle believed that the draft NSA's solution was a strong one, specifically in relation to the three core concerns CFIUS identified: data security, software assurance, and content assurance. Counsel noted that there had been nearly two years of work put into that solution, and that it would be helpful to know why the government believed the solution was deficient. None of the government attendees at the March 23, 2023 meeting addressed this question in any detail. Rather, Mr. Reissaus reiterated the U.S. government's conclusory position that even with the provisions put in place in the draft NSA, the "most effective" method to address the government's concerns would be divestment. Mr. DeBacker stated that the government would not otherwise get into the specifics of what was discussed internally by the government over the preceding several months.

Mr. DeBacker also asked how the Company was navigating this matter with the Chinese government, given the Chinese government's prior objection to divestiture. He specifically asked whether either a passivity structure over the U.S. business of TikTok (which DOJ and Treasury had previously made clear was *not* acceptable to CFIUS) or divestiture would be characterized as a forced sale. Counsel confirmed that Chinese regulatory restrictions would likely be an obstacle, and asked why this information was "new or surprising" to CFIUS given the history of this matter. Mr. DeBacker confirmed that it was not new or surprising, and reiterated (i) that the previous conversation on March 6, 2023 made clear that from the government's standpoint, the only workable solution was divestment and source code migration, and (ii) that it now sounded like divestment and source code migration might be infeasible. Counsel responded that the government's position as articulated on March 6, 2023 was "unmoored from reality," and that Mr. DeBacker's characterization was correct—*i.e.*, *the divestiture and source code migration was not feasible*. Nonetheless, counsel agreed to take the issues back and to explore what further proposal the Company could realistically make under the circumstances. Counsel also repeated the Company's request to meet with the Deputies, and was again rebuffed.

APP-421

Following this meeting, on April 27, 2023, counsel sent the following email to DOJ and Treasury:

From: Fagan, David
Sent: Thursday, April 27, 2023 7:13 PM
To: 'Brian.Reissaus@treasury.gov' <Brian.Reissaus@treasury.gov>; Andrew.Fair@treasury.gov; Devin.DeBacker@usdoj.gov; Evan.Sills@usdoj.gov; Tyler.Wood@usdoj.gov; Winnie.Tsang@treasury.gov; Sarah.Oldham@treasury.gov; David.Newman2@usdoj.gov; Eric.S.Johnson@usdoj.gov; Nayla.Kawerk@treasury.gov; Theodore.Posner@treasury.gov
Cc: Michael.Leiter@skadden.com
Subject: RE: CFIUS Case. No. 20-100: Status

Business Confidential - Pursuant to 50 U.S.C. Section 4565; Protected from Disclosure Under 5 U.S.C. Section 4565

Treasury and DOJ colleagues -

We wanted to provide the Committee with an update on the work that ByteDance has been undertaking to address the issues that we discussed in our meetings on March 6 and March 23. As we have discussed, both the Committee's position on ownership and its articulated position on source code raise extremely complex commercial and legal challenges. Nevertheless, ByteDance has been exploring solutions to both issues. There are active workstreams ongoing with the goal of being able to make a presentation to CFIUS later in May on potential solutions. To be sure, that does not mean that ByteDance agrees with the articulated positions, or that a divestiture or source code migration will even be practical commercially or because of the restrictions of Chinese law. It does mean, however, that ByteDance is working on the issues in good faith, and intends to present proposals on each prong in May. We currently think that will likely be the middle-to-latter half of the month, but will keep you apprised.

Best regards,

Mike and David

David Fagan

Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5291 | M + 1 703 967 6940
dfagan@cov.com
https://hyperlink.services.treasury.gov/agency.do?origin=www.cov.com

COVINGTON

May 23, 2023 In-Person Meeting

As promised in its April correspondence, on May 23, 2023, counsel and technical experts for the Company met at the Department of the Treasury with Mr. Rosen, yourself, and other members of your respective teams to discuss possible TikTok governance changes and source code migration that could be realistically achieved.

The Company's presentation started by noting that the positions of the U.S. government and the Chinese government were flatly incompatible, putting the company in an impossible position. The Company then set forth the practical challenges to addressing the government's divestiture position. The Company noted that even narrowing the government's divestiture demand to TikTok U.S. Data Security would be complicated economically, since TikTok U.S. Data Security was a backend company without an independent revenue stream; the change in control would impact existing agreements with third parties (such as agreements for music); the Company did not have separate intellectual property for TikTok U.S. Data Security; the business of TikTok U.S. Data Security would simply be as a *de facto* vendor to the rest of TikTok; it was not clear who would buy the business given the foregoing, and even then, regulatory approval—including with respect to the algorithm—would be uncertain. If the compelled divestiture were widened to include TikTok Inc., any sale would almost certainly be blocked by the Chinese government; the divestiture would break interoperability, forcing TikTok U.S. "to become an

APP-422

island" where U.S. users would have an experience detached from the rest of the global internet (not unlike app services offered in China); and it would so substantially increase business costs through duplication that, again, it was highly uncertain that there would be any buyers. The slides also specifically noted that the effect of these challenges would be a ban of TikTok in the United States:
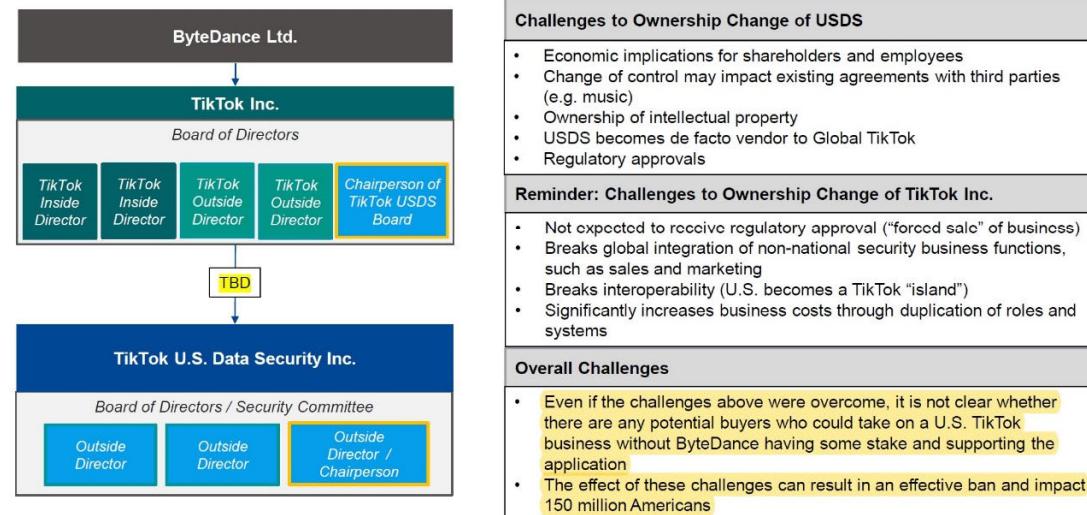
The remainder of the presentation focused in detail on source code, including the existing source code and content assurance plans under Project Texas. The Company then presented an additional proposal for potential migration out of China for source code related to video promotion and filtering ("VPF"), explaining that it could be accomplished in six months to a year, subject to certain conditions. The Company never received *any* feedback from you or anyone on your team on this proposal, despite several attempts by counsel to elicit a response.

September 8, 2023 Meeting

In late August, the agencies agreed to another meeting with the Company, which occurred on September 8, 2023. The meeting included *another* technical discussion of the challenges of migration, including specifically addressing challenges in "forking" the code. In addition to reviewing its proposal on migration of VPF software, which was presented on May 23, 2023, the Company set forth its analysis of the "alternative" demanded by the government on March 6, 2023, *i.e.*, a full migration. The Company provided a detailed breakdown of the government's proposed migration with respect to the full "stack" of the TikTok source code—*i.e.*, with the source code divided into its constituent parts: content moderation, recommendation engine, VPF (and related backend), and all internal tools.

The Company explained that ***even if*** the government's contemplated divestiture were not blocked by the Chinese government's export control restrictions, which was a baseline reality, the U.S. government's proposal had significant challenges, including "complexity in managing risk of incompatible systems with the independent development of [an] alternative recommendation engine." Moreover, counsel explained, it would not be possible to move all development to the United States, and even moving it to other countries where TikTok operates would pose a significant challenge to find qualified engineers. As a practical matter, any such migration would mean that all relevant engineers currently located in China would need to move to those other countries, and they would still need to access internal reference documents and tools.

Again, the Company sought clarity from the government on *what precisely* was deficient with the Company's proposed NSA. As counsel explained, the draft NSA already contemplated migration of the content assurance system plus full access to source code by independent highly qualified third parties approved by CFIUS. Again, the government failed to articulate any particularized deficiencies with the mitigations set forth in the draft NSA.

Nevertheless, the Company indicated that it was willing to explore even broader migration of source code, subject to conditions, and it provided estimated timelines for such a broader migration. While the VPF migration could be completed within a year, other systems would take longer, and the Company explained that the recommendation engine systems and models and internal tools would take at least two years to move. Importantly, counsel explained—yet again— that among the conditions of its proposal was Chinese export control regulatory approvals, and the Company had no reason to think the Chinese government had changed its earlier position.

Again, the Company never received a response from the government on this presentation. Counsel for the Company pursued additional meetings, and understood from these communications in November 2023 that there was some discussion and effort on the government's side to arrange a meeting on governance. But that meeting never materialized, and the government never made any effort to respond or engage until your March 14, 2024 email.

> ***C. Your email from March 14 concludes:*** *"We would ask that you provide us with an update on the status of your client's response to our position and on the ongoing measures that TikTok is taking to address the national security concerns we have raised. We would like to set a time within the next two weeks to update Paul and myself (and other Treasury and DOJ officials) on this matter in person."*

> ***Your email from March 18 then states:*** *"If your client is unwilling — or perhaps unable — to provide voluntarily the requested update on the efforts to address the national security harms that we've raised, that would be useful to have confirmed. Absent hearing from you, we will proceed accordingly."*

Neither your email from March 14 nor your follow up from March 18 acknowledges the foregoing history, and it is confounding that your emails ask us for a response to the government's position when (1) the Company has provided detailed responses to the government's position over

the course of multiple meetings; and (2) the government has refused to speak with us for months at a time and to this date has not provided any feedback on the Company's proposals on source code migration from May 23 and September 8, 2023.

We further note that while CFIUS itself has refused to engage with the Company for many months, your email of March 14, 2024 arrived the day *after* the House passed H.R. 7521 (just as your March 6, 2023 communication appears to have been coordinated with the introduction of the RESTRICT Act), which, if enacted, would prohibit distributing, maintaining, or providing internet hosting services for TikTok or other ByteDance apps. It was publicly reported that DOJ briefed members of Congress in advance of a vote on the bill, and that the briefing included a document that stated, among other things, that CFIUS has "limits that make it challenging to effectuate" a divestment of TikTok from ByteDance.[5]

Based on our four and a half years of engagement on this matter and decades of CFIUS experience, we are confident that the CFIUS framework provides a constructive forum to discuss and address the government's asserted concerns, despite the absence of a record to support CFIUS jurisdiction. CFIUS can only serve this function, however, when the law and CFIUS regulations are followed and both sides are engaged in good-faith discussions, as opposed to political subterfuge, where CFIUS negotiations are misappropriated for legislative purposes. We fear, based on the foregoing record set forth in this letter just related to the last year, let alone the U.S. government record of the three and a half years before that, that CFIUS has become compromised by political demagoguery in this matter. Nonetheless, we and the Company remain committed to any process that honors the law and CFIUS norms. In this vein, we look forward to a meaningful, re-started engagement with CFIUS at your convenience.

Best regards,

By: _____

Michael E. Leiter
Skadden, Arps, Slate, Meagher &
Flom LLP
1440 New York Avenue, N.W.
Washington, DC. 20005-2111

By: _____

David Fagan
Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956

Cc: Paul Rosen, Assistant Secretary of the Treasury for Investment Security

Enclosure

---

[5] David Shepardson, "TikTok divestment bill would give government stronger legal position, US DOJ says," Reuters (Mar. 8, 2024), https://www.reuters.com/world/us/bytedance-tiktok-divestment-bill-would-give-government-stronger-legal-position-2024-03-08/; David Shepardson (@davidshepardson), X (Mar. 8, 2024 5:22 PM), https://twitter.com/davidshepardson/status/1766228113887768931.

EXHIBIT A

DRAFT NATIONAL SECURITY AGREEMENT

This NATIONAL SECURITY AGREEMENT ("**Agreement**") is made as of [date] (the "**Effective Date**"), by and among: (i) ByteDance Ltd., a Cayman Islands exempted company ("**ByteDance**"); (ii) TikTok Ltd., a Cayman Islands exempted company ("**TikTok Ltd.**"); (iii) TikTok Inc., a California corporation ("**TikTok Inc.,**" and together with ByteDance, TikTok Ltd., and, upon its joinder to this Agreement, TikTok U.S. Data Security Inc. ("**TTUSDS**"), the "**Transaction Parties**"); and (iv) [•], (together, the "**CFIUS Monitoring Agencies**," or "**CMAs**," and the CMAs together with the Transaction Parties, the "**Parties**") on behalf of the Committee on Foreign Investment in the United States ("**CFIUS**").

RECITALS

WHEREAS, CFIUS received written notification, dated May 27, 2020, including all information and documentary materials subsequently submitted in connection therewith, pursuant to Section 721 of the Defense Production Act of 1950, as amended ("**Section 721**"), of a transaction that was the subject of CFIUS Case 20-100;

WHEREAS, the transaction involved the merger of a wholly owned subsidiary of ByteDance with and into musical.ly ("**Musical.ly**"), a Cayman Islands exempted company, on November 23, 2017 (the "**Transaction**");

WHEREAS, CFIUS determined that the Transaction constituted a "covered transaction" for purposes of Section 721;

WHEREAS, CFIUS undertook a review and investigation of the effects of the Transaction on the national security interests of the United States, including a risk-based analysis, as required by Section 721, and determined that there were risks to the national security of the United States that arose as a result of the Transaction;

WHEREAS, CFIUS informed ByteDance, by a letter dated July 30, 2020, that CFIUS had not identified any mitigation options that would resolve CFIUS's concerns regarding the national security risks arising from the Transaction;

WHEREAS, pursuant to Section 721, CFIUS referred the Transaction to the President of the United States;

WHEREAS, the President of the United States determined that provisions of law, other than Section 721 and the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), do not provide adequate and appropriate authority to protect the national security of the United States;

WHEREAS, the President of the United States issued the Order of August 14, 2020, Regarding the Acquisition of Musical.ly by ByteDance Ltd. (85 Fed. Reg. 51,297 (Aug. 19, 2020)) ("**August 14 Order**") prohibiting the acquisition by ByteDance of Musical.ly to the extent that Musical.ly or any of its assets is used in furtherance or support of, or relating to, Musical.ly's

APP-427

activities in interstate commerce in the United States ("**Musical.ly in the United States**"), prohibiting ByteDance's direct or indirect ownership of any interest in Musical.ly in the United States, and in order to effectuate the August 14 Order, on such written conditions as CFIUS may impose, requiring ByteDance, its subsidiaries, affiliates, and Chinese shareholders to divest all interests and rights in: (i) any tangible or intangible assets or property, wherever located, used to enable or support ByteDance's operation of the TikTok application in the United States, as determined by CFIUS; and (ii) any data obtained or derived from TikTok application or Musical.ly application users in the United States (clauses (i) and (ii), collectively, the "**Divestment**");

WHEREAS, the August 14 Order authorizes CFIUS, until such time as the Divestment is completed and verified to the satisfaction of CFIUS, to implement measures it deems necessary and appropriate to verify compliance with the August 14 Order and to ensure that the operations of the TikTok application are carried out in such a manner as to ensure protection of the national security interests of the United States;

WHEREAS, ByteDance filed a petition for review of the August 14 Order and the related CFIUS actions in the U.S. Court of Appeals for the District of Columbia Circuit on November 10, 2020 (the "**Petition**"), and the adjudication of such action has been held in abeyance pending ongoing discussions with CFIUS;

WHEREAS, without admission of fault or liability, ByteDance and the CMAs, on behalf of CFIUS, are entering into this Agreement with the understanding that this Agreement will resolve the findings and concerns reflected in the August 14 Order, including the aforementioned Petition; and

WHEREAS, each of the Transaction Parties as of the Effective Date affirms that it is acknowledging and entering into this Agreement with the understanding that: (i) there is no presumption that a waiver or exception will be granted to any provision of this Agreement; and (ii) failure to abide by this Agreement is subject to all remedies available to the U.S. Government ("**USG**"), including those stated herein;

NOW, THEREFORE, pursuant to applicable law, including Section 721 and the August 14 Order, the CMAs, acting on behalf of CFIUS, hereby enter into this Agreement with the Transaction Parties:

ARTICLE I

DEFINITION OF TERMS

Definitions. As used in this Agreement, capitalized terms shall be defined as set forth below; *provided* that capitalized terms used in this Agreement and not defined in this Article I shall have the meanings assigned to them elsewhere in the Agreement:

1.1   "**Access**" means to, or the right or ability to: (1) enter a physical space ("**Physical Access**"); or (2) obtain, read, copy, edit, divert, release, affect, alter the state of, or otherwise

view the subject data or systems in any form, directly or indirectly, whether remotely or electronically, including through information technology ("**IT**") systems, cloud computing platforms, networks, security systems, software, and hardware ("**Logical Access**"). Access shall be construed broadly to include rather than exclude considered conduct.

1.2 "**Affiliate**" or "**Affiliates**" means, with respect to a specified Person, another Person that directly or indirectly, through one or more intermediaries, Controls, is Controlled by, or is under common Control with the Person specified; *provided* that for purposes of this Agreement, (i) TTUSDS and its Personnel shall not be considered Affiliates of ByteDance, and (ii) third-party shareholders of ByteDance also shall not be considered Affiliates of ByteDance.

1.3 "**Architecture Diagrams**" means one or more high-level outlines, using functional blocks and line illustrations for graphical description, of the end-to-end system concept and relationships, constraints, and boundaries between components for or supporting the TikTok U.S. App or TikTok U.S. Platform and that include detailed explanations or annotations identifying: (1) operational functionality; (2) ownership, control, and Logical Access rights, capabilities, and limitations; and (3) system input and output capabilities and limitations.

1.4 "**CFIUS Restricted Persons**" means, wherever located: (1) the government of any country identified in 22 C.F.R. §§ 126.1(d)(1) and (2) (each, a "**CFIUS Restricted Country**") or any department, agency, or instrumentality thereof; (2) any Person organized, domiciled, headquartered, or with its principal place of business in a CFIUS Restricted Country; (3) any natural Person with nationality of a CFIUS Restricted Country who is not also (a) a U.S. citizen, (b) lawfully admitted for permanent residence as defined by 8 U.S.C. § 1101(a)(20), or (c) a protected individual as defined by 8 U.S.C. § 1324b(a)(3); or (4) any natural Person working or residing in a CFIUS Restricted Country. CFIUS Restricted Persons include any Person who, to the best of the Transaction Parties' knowledge based on information reasonably available to them, is owned, Controlled by, or acting on behalf of a CFIUS Restricted Person; *provided, however*, that for purposes of this Agreement, TTUSDS shall not be considered a CFIUS Restricted Person.

1.5 "**Content Delivery Network**" or "**CDN**" means servers and related infrastructure that is used for the delivery of static and live content to the TikTok U.S. App (including livestreaming and communication services) that require geographical distribution to address latency issues and cannot reside exclusively within the TTP's secure cloud infrastructure.

1.6 "**Content Promotion and Filtering**" means the promotion or filtering of content on the TikTok U.S. App outside the context of the Recommendation Engine, either through human intervention or technical measures, including relevant algorithms, rules, logic and guidelines.

1.7 "**Control**" (including the terms "**Controlled by**" and "**under common Control with**") means the power, direct or indirect, whether or not exercised, to determine, direct, or decide important matters affecting a Person, whether by ownership of equity interests, contract, or otherwise.

APP-429

1.8   "**Creator**" means a TikTok U.S. User who has a contractual relationship with TikTok Inc. or one of its Affiliates (other than contractual relationships applicable to all TikTok U.S. Users, e.g., acceptance of the Terms of Service) for the purpose of promoting the individual or his or her brand, to earn revenue from his or her creative output, or for another promotional purpose that is intended to advance the commercial interests, following, or brand of the individual.

1.9   "**Data Flow Diagrams**" means one or more high-level outlines, using functional blocks and line illustrations for graphical description and detailed explanation, of the end-to-end flow of data to support or operate the TikTok U.S. App or TikTok U.S. Platform, including what data or information will be input and output from the system, where the data or information will come from and go to, and where the data or information will be stored. Data Flow Diagrams shall also identify: (1) the operation performed; and (2) ownership, control, and Logical Access rights, capabilities, and limitations.

1.10   "**Dedicated Transparency Center**" or "**DTC**" means physical facilities, processing resources, and network storage that are established by ByteDance in the DTC Approved Countries for the express purpose of enabling security inspections, reviews, and verification of the Source Code and Related Files by TTUSDS, the TTP, and other third parties pursuant to this Agreement.

1.11   "**Excepted Data**" means each of the following:

(1)   data that Creators affirmatively authorize to be shared, or otherwise initiate the sharing, with TikTok Inc. or its Affiliates for the purpose of advancing the Creators' commercial position on the TikTok U.S. App;

(2)   data fields in the formats specified in Annexes A and B hereto that are: (i) categories of engineering and business data metrics or (ii) categories of interoperability data, respectively;

(3)   data fields in the formats specified in Annex C that are categories of e-commerce data for transactions conducted through the TikTok U.S. App and TikTok U.S. Platform ("**E-Commerce Data**"), *provided* that:

(i)   the data is necessary for commercial purposes related to the sale of the goods and services initiated by the TikTok U.S. User, including the data required to be shared with third parties involved in the transaction;

(ii)   prior to the use of said data as E-Commerce Data, a TikTok U.S. User is notified that such data may be shared outside the United States with ByteDance and affiliates for the purposes described in the aforementioned subparagraph; and

(iii)   after one (1) year from the date of sale, E-Commerce Data shall be maintained exclusively by TTUSDS except when the data is required to fulfill an

4

APP-430

authorized e-commerce function as described in Annex C, which may be modified in consultation with the Security Committee through a protocol approved by the CMAs;

(4)   hashes of username, phone number, email address, or OpenID, solely for the purpose of determining whether a user should be routed to the TikTok U.S. Platform, shall not be considered Protected Data; and

(5)   additional categories of data, as approved by the CMAs, in their sole discretion pursuant to Section 11.1

1.12   "**Executable Code**" means the binary, machine-readable Software code derived from Source Code and Related Files.

1.13   "**Existing Network Diagram**" means a diagram providing a complete description of the Transaction Parties' network topology, router and server technology of its U.S. network and any U.S. networks of its Affiliates for operating or supporting the TikTok U.S. App or TikTok U.S. Platform as of the Effective Date.

1.14   "**Key Management**" means any Personnel involved in the leadership of TTUSDS, including the general manager, president, chief executive officer, chief information officer, chief technology officer, chief operating officer, general counsel, or equivalent positions (to the extent that such positions exist), such other officers who directly report to the TTUSDS Board or the TTUSDS general manager or equivalent, security leadership roles, and any Personnel of TTUSDS designated as Key Management by the CMAs in their sole discretion pursuant to Section 5.1.

1.15   "**Lawful U.S. Process**" means U.S. federal, state, or local orders or authorizations, and other orders or legal process, statutory authorizations, or certifications from U.S. federal, state, or local law enforcement officials for Access to or disclosure of information, user communications, or content.

1.16   "**Malicious Code**" means code that facilitates the circumvention of this Agreement, facilitates surveillance by unauthorized parties, or delivers nefarious applications or programs to the devices of TikTok U.S. Users; and/or software or firmware intended to perform an unauthorized process that will have adverse impacts on the confidentiality, integrity, or availability of a system including a virus, worm, trojan horse, spyware, forms of adware, or any other code-based entity that infects a host.

1.17   "**Master Services Agreement**" or "**MSA**" means the master services agreement among ByteDance, TTUSDS, and the TTP (the first TTP being Oracle Corporation ("**Oracle**")).

1.18   "**NIST**" means the National Institute of Standards and Technology.

1.19   "**Person**" means any individual or entity.

1.20   "**Personal Identifier Information**" means an individual's: (1) full name (last, first, middle name); (2) all other names and aliases used; (3) business address; (4) country and

city of residence; (5) date of birth; (6) place of birth; (7) U.S. Social Security number (where applicable); (8) national identity number, including nationality, date and place of issuance, and expiration date (where applicable); (9) U.S. or foreign passport number (if more than one, all must be fully disclosed), nationality, date and place of issuance, and expiration date and, if a U.S. visa holder, the visa type and number, date and place of issuance, and expiration date; and (10) dates and nature of foreign government and foreign military service (where applicable), other than military service at a rank below the top two non-commissioned ranks of the relevant foreign country.

1.21 "**Personnel**" means any employee, director, officer, manager, agent, contractor, or other representative of an entity, and includes the respective successor or assigns of the foregoing.

1.22 "**Protected Data**" means any data collected from a TikTok U.S. User, including: (1) user data (including username, password, email address, phone number, nickname, birth date or age, profile thumbnail, biographical information, genetic or biometric data or information, appearance, device contacts list, and any third-party social media credentials, list of third-party applications installed on the same device as the TikTok U.S. App, or payment account information); (2) user content (including videos, music, pictures, articles, hashtags, captions, comments, direct messages, and other material uploaded by users including private or unpublished content); (3) behavioral data (including user interaction with content, such as likes given, likes received, not interested, video playtime, shares, follows, followers, block list, favorites, downloads, log-in history, browsing history, search history, keystroke patterns and rhythms, and purchase history); (4) any data that is collected on U.S. user interaction with content on the TikTok U.S. Platform as an input into the Recommendation Engine, including video completion, not interested markings, and video viewing time, ("**User Interaction Data**"); (5) device and network data (including Internet Protocol ("**IP**") address, cookie data, device identifiers, MAC address, mobile carrier, network settings, time zone settings, app and file names, device clipboard, device contacts, device calendars, device media, source of user, Android ID, Apple ID for Advertisers, Google Advertising ID, any other ID for Advertisers, device model and characteristics, operating system ("**OS**"), list of installed apps, system language and region, and geographic location, such as the city, state, country, or GPS coordinates of the device's location); (6) any other personally identifiable information; and (7) any other information provided by or derivative of TikTok U.S. Users in connection with their use of the TikTok U.S. App. Protected Data includes all of the foregoing even if de-identified, anonymized, or aggregated but shall not include Excepted Data or Public Data. TikTok U.S. Platform systems log data that has had all Protected Data removed by the TTP shall not be Protected Data.

1.23 "**Public Data**" means data that is generally accessible to users of the TikTok U.S. App, including videos, comments, and similar user content and includes each of the following:

(1) feature categories as specified in Annex E;

(2) any content that TikTok U.S. Users affirmatively decide to make public;

(3) any hash of Public Data; and.

(4) additional feature categories added pursuant to Section 11.2.

1.24 "**Recommendation Engine**" means the algorithms and related data models used by the TikTok U.S. App and TikTok U.S. Platform to rank content and select content for recommendation to TikTok U.S. Users, including their Source Code and Related Files, such as machine learning processes, statistical weights and parameters, and outputs. For the avoidance of doubt, the Recommendation Engine does not include the Content Promotion and Filtering algorithms.

1.25 "**Resident Sole U.S. Citizen**" means an individual who holds U.S. citizenship and currently has, and maintains for the duration of his or her responsibilities in connection with this Agreement, residency in the United States as determined by meeting the substantial presence test set forth in 26 U.S.C. § 7701(b)(3), and who is not a citizen of any other country.

1.26 "**Resident U.S. Citizen**" means an individual who holds U.S. citizenship and currently has, and maintains for the duration of his or her responsibilities in connection with this Agreement, residency in the United States as determined by meeting the substantial presence test set forth in 26 U.S.C. § 7701(b)(3).

1.27 "**Software**" means a set of instructions that are generated from source code and used to operate electronic devices and execute specific tasks on a device or a system, including executable code, tools, platforms, and related user manuals.

1.28 "**Source Code and Related Files**" means: (1) all of the actual, human-intelligible Software code, including files, libraries, data schemas and algorithms from ByteDance and its Affiliates used to operate the TikTok U.S. App or TikTok U.S. Platform; and (2) any other documentation, specifications, and artifacts from ByteDance and its Affiliates that are used to design, develop, maintain, modify, operate, improve, or define the behavior of the TikTok U.S. Platform or the TikTok U.S. App. For the avoidance of doubt, "Source Code and Related Files" shall not include (1) or (2) when developed by TTUSDS.

1.29 "**Source Code Review Diagrams**" means one or more high-level outlines, using descriptive functional blocks and line illustrations for graphical description, of the process for reviewing Source Code and Related Files that identify: (1) the operation performed; (2) who among the Transaction Parties or the TTP has obligations or actions to perform; and (3) who among the Transaction Parties or TTP has ownership, Logical Access, or control.

1.30 "**SPAC Transaction**" means the consummation of a transaction or series of transactions (whether by merger, consolidation, or transfer or issuance of equity interests or otherwise) whereby a special purpose acquisition company acquires all of the equity interests of a company (or any surviving or resulting company) or a transaction having a similar effect.

1.31 "**Test Accounts**" means accounts established by the Transaction Parties and verified and approved by the TTP as accounts not associated with any individual for the purpose

of testing operational functionality and enabling continued innovation and refinement of user features of the TikTok U.S. App and TikTok U.S. Platform.

1.32   "**TikTok Global App**" means each of the following, in their current and future versions and as the service may evolve:

(1)   the TikTok-branded application(s), including any regional or other jurisdiction-specific versions, that are accessible by the public through an online application store (e.g., one offered by Apple, Google, or Amazon) or an equivalent method of accessing the application and that allows users to consume, create, share, and otherwise interact with content; and

(2)   the TikTok web application(s) that are used to provide web browser users with a TikTok product experience similar to the product experience provided through the TikTok-branded application(s) described in clause (1) of this definition on mobile devices.

1.33   "**TikTok U.S. Application**" or "**TikTok U.S. App**" means all versions of the TikTok Global App provided to, or accessible by, TikTok U.S. Users.

1.34   "**TikTok U.S. Platform**" means the infrastructure, including the IT systems, cloud computing platforms, servers, networks, security systems, and equipment (software and hardware), and all related services and program elements that host, operate, maintain, deploy, support, and run the service and storage facilities for the TikTok U.S. App. For avoidance of doubt, the Recommendation Engine shall be contained and deployed from within the TikTok U.S. Platform.

1.35   "**TikTok U.S. User**" means:

(1)   an individual signing into the TikTok Global App through an account that, at the time of registration, was attributable to the United States based upon any of the following means (with respect to Sections 1.32(1)(i)–(iv), in order of priority):

(i)   Country code of the device subscriber identity module ("**SIM**") card;

(ii)   IP Address;

(iii)   Mobile Country Code associated with the mobile subscription of the device; or

(iv)   OS/System Region (i.e., obtained via an application programming interface ("**API**") call provided by the OS (either Android or iOS), which returns a country code);

(2)   an individual signing into the TikTok Global App through an account that has been designated a "TikTok U.S. User" account pursuant to Section 11.3; or

(3)   for users who are not signing into the TikTok Global App with a registered account, a device that first accesses the TikTok Global App from an IP address located in the United States.

(4)   For the avoidance of doubt, Test Accounts shall not be considered TikTok U.S. Users.

1.36   "**Trust and Safety Moderation**" means the removal or downgrading of content or user accounts that are viewable or eligible for recommendation on the TikTok U.S. App, either through technical measures or human review, in order to meet trust and safety guidelines. Trust and Safety Moderation excludes Content Promotion and Filtering.

1.37   "**Trusted Technology Provider**" **or** "**TTP**" means Oracle in its capacity as the TTP, or any successor TTP, in each case operating under an MSA consistent with the requirements of Section 8.2.

1.38   "**United States**" or "**U.S.**" means the several States, the District of Columbia, and any territory or possession of the United States.

ARTICLE II

FORMATION OF TIKTOK U.S. DATA SECURITY INC.

2.1   Formation of TikTok U.S. Data Security Inc. By no later than one-hundred and eighty (180) days following the Effective Date (the "**Operational Date**"), ByteDance shall establish TTUSDS as a wholly owned subsidiary of TikTok Inc. that is incorporated in the United States. The Transaction Parties may request an extension of the Operational Date no later than one-hundred and sixty-six (166) days following the Effective Date, in which case the Transaction Parties shall submit to the CMAs a written request that includes a summary of the actions taken to date, the reason for the delay, and the requested new Operational Date. The CMAs may non-object, non-object with predicate conditions, or object to the request for an extension in their sole discretion. In the event that the CMAs non-object with predicate conditions to the request, the Operational Date shall be extended only if the Transaction Parties meet the specified conditions to the satisfaction of the CMAs in the CMAs' sole discretion. In the event that the CMAs object to the request, the Operational Date shall not be extended. If the CMAs do not either object or non-object with predicate conditions to the request within seven (7) days of receipt, the lack of action shall constitute a non-objection.

2.2   Headquarters. By no later than the Operational Date and at all times thereafter, ByteDance shall ensure that TikTok Inc. and TTUSDS maintain their respective headquarters offices exclusively in the United States and that TTUSDS's offices are not co-located with any offices of ByteDance or its Affiliates without prior written approval of the CMAs. Immediately following the Operational Date, TTUSDS shall also ensure that its headquarters offices are maintained in the United States and that its offices are not co-located with any offices of ByteDance or its Affiliates without prior written approval of the CMAs. Following the

Operational Date, TTUSDS shall ensure that only its Personnel are responsible for the day-to-day operations and management of TTUSDS's business.

2.3   TTUSDS Joinder. By no later than the Operational Date, ByteDance shall ensure that TTUSDS joins this Agreement by submitting to the CMAs a joinder agreement signed by a duly authorized representative of TTUSDS that is in the form at Annex D.

2.4   CFIUS Functions. By no later than the Operational Date and at all times thereafter, the Transaction Parties shall ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all of the Personnel related to the following aspects of the TikTok U.S. App's operations (collectively, the "**CFIUS Functions**"):

(1)   overseeing the storage and protection of Protected Data, including through TTUSDS's activities pursuant to the MSA;

(2)   facilitating and assisting with the TTP's receipt and inspection of Source Code and Related Files via the DTC, as well as TTUSDS's and the TTP's deployment of Executable Code;

(3)   TikTok U.S. App trust and safety operations and functions that require Access to any Protected Data (except as otherwise expressly provided for in this Agreement);

(4)   content, user, and advertising operations, including Content Promotion and Filtering, that require Access to any Protected Data;

(5)   identifying and implementing remediations for the Recommendation Engine in response to the review by the TTP pursuant to this Agreement;

(6)   overseeing, authorizing, and documenting the sale or transfer of Protected Data to any third parties, to the extent that such sale or transfer is permitted under this Agreement; and

(7)   maintaining primary responsibility for ensuring day-to-day compliance with this Agreement.

2.5   Enabling TTUSDS. By no later than the Operational Date, and to ensure that TTUSDS can effectively and independently perform the CFIUS Functions, ByteDance shall, and shall ensure that its Affiliates:

(1)   take all necessary actions to ensure that all commercial agreements with third parties for the operation and delivery of the TikTok U.S. App and TikTok U.S. Platform are transferred, assigned, licensed, or otherwise contributed, as applicable, to TTUSDS;

(2)   subject to Section 5.4, transfer the employment agreements of all Personnel responsible for performing the CFIUS Functions to TTUSDS;

APP-436

(3)   enter into a license and service agreement with TTUSDS, to be developed in coordination with the CMAs and the TTP to ensure that the terms of such license and service agreement are consistent with this Agreement, that:

(i)   ensures TTUSDS has all necessary rights to ByteDance technology, including Source Code and Related Files and all updates thereto, Executable Code, and other Software required to operate and manage the TikTok U.S. App and TikTok U.S. Platform, for the purposes set forth in this Agreement;

(ii)   provides TTUSDS with support to perform the CFIUS Functions; and

(iii)   provides that in the event of a conflict between the terms of such license and service agreement and this Agreement, the terms of this Agreement shall prevail; and

(4)   sub-license to TTUSDS, or arrange for new licenses for TTUSDS to, all third-party Software and technologies for which ByteDance is a licensee that are necessary to operate and manage the TikTok U.S. App and TikTok U.S. Platform.

2.6   <u>Formation and Operational Plan</u>. ByteDance shall submit a plan to the CMAs within fourteen (14) days following the Effective Date that describes the steps ByteDance will take to:

(1)   ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all Personnel related to the CFIUS Functions;

(2)   contribute, assign, or license to TTUSDS, as applicable, all assets necessary to comply with this Agreement; and

(3)   ensure that TTUSDS will become operational by the Operational Date, which at a minimum means that TTUSDS can manage its day-to-day operations and perform the CFIUS Functions as set forth in this Agreement separate and apart from ByteDance and its Affiliates.

2.7   <u>TTUSDS Independence</u>. By no later than the Operational Date and at all times thereafter, ByteDance shall not play any role in or make any attempt to influence, determine, direct, or decide the operations, management, or leadership of TTUSDS, except as otherwise expressly provided for in this Agreement. ByteDance shall ensure that none of its Affiliates plays any role in or makes any attempt to influence, determine, direct, or decide the operations, management, or leadership of TTUSDS, except as otherwise expressly provided for in this Agreement.

2.8   <u>TTUSDS Funding</u>. ByteDance shall provide sufficient financial resources to enable TTUSDS to fully perform the CFIUS Functions and fulfill its obligations under this Agreement. TTUSDS shall promptly notify the Third-Party Monitor and CMAs if TTUSDS

believes, in its sole discretion, that it lacks sufficient funds to perform the CFIUS Functions and fulfill its obligations under this Agreement. The Transaction Parties shall provide semi-annual updates to the Third-Party Monitor and CMAs regarding the budgeting and funding of TTUSDS.

2.9   Ownership of TTUSDS. At least seven (7) days prior to entering into any agreement or completing any transaction through which: (1) any Person other than TikTok Inc. will acquire a direct economic or voting interest in TTUSDS; or (2) there will be a greater than five percent (5%) change to the ownership of the indirect economic or voting interests in ByteDance, TikTok Inc., or TTUSDS as of the Effective Date, the Transaction Parties shall provide written notification to the CMAs of the identity of the Person to own the interest, the percentage and nature of the interest to be owned, and all relevant transaction documents and side agreements; *provided, however*, that prior notice of any transaction described in Section 2.9(2) shall not be required if such transaction would not involve a change in the direct economic or voting interests in TikTok Inc., TTUSDS, or any other subsidiary of ByteDance, and ByteDance is a publicly listed company at the time of such transaction. The Transaction Parties shall also submit to the CMAs a quarterly summary capitalization table of ByteDance identifying all shareholders holding a more than one percent (1%) equity interest or voting interest in ByteDance as of the end of the quarter.

ARTICLE III

GOVERNANCE OF TIKTOK U.S. DATA SECURITY INC.

3.1   TTUSDS Board Composition. The Transaction Parties shall ensure that TTUSDS is at all times governed by a board of directors (the "**TTUSDS Board**") of three (3) directors who: are Resident Sole U.S. Citizens, unless otherwise approved by the CMAs; have no current or prior employment, or contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates; have strong credentials in national security or extensive experience in IT, cybersecurity, or data security; and have, or are eligible for, a U.S. personnel security clearance (the "**Security Directors**").

(1)   The Transaction Parties shall ensure that the composition of the TTUSDS Board is limited exclusively to the Security Directors. The Transaction Parties shall designate, subject to CMA non-objection concurrent with the appointment process in Section 3.2, one of the Security Directors as Chair of the TTUSDS Board (the "**TTUSDS Chair**"), and a second Security Director as Chair of the Security Committee established pursuant to Section 3.8. For the avoidance of doubt, the Transaction Parties may appoint the TTUSDS Chair as chair of the Security Committee. Subject to CMA approval, the Transaction Parties shall be able to set term limits and/or stagger the terms for each Security Director, the expiration of a Security Director term being treated as a vacancy pursuant to Section 3.09 of the Agreement, including for purposes of triggering the timing requirements for replacements.

3.2   Initial TTUSDS Board Appointments. The Transaction Parties shall ensure that no Security Director is appointed or otherwise becomes a director without the prior non-objection of the CMAs. At least [X] days prior to the Operational Date, the Transaction Parties shall submit to the CMAs complete Personal Identifier Information, a *curriculum vitae* or similar

professional synopsis, contact information, and any other information requested for each Security Director nominee for the CMAs to assess whether the nominee can effectively perform the functions set forth in this Agreement. The Transaction Parties shall ensure that the CMAs may, at their request, interview the Security Director nominees. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about the Security Director nominees, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to one or more Security Director nominees, the Transaction Parties shall nominate a different candidate within twenty-one (21) days following receipt of any such objection, subject to the same procedures as the initial nomination. The Transaction Parties shall ensure that a Security Director is appointed for each Security Director position on the TTUSDS Board following the non-objection of the CMAs by no later than the Operational Date. After the Operational Date, if all the board seats are not filled, the Transaction Parties shall ensure that any initial Security Director nominee is appointed within three (3) days following the non-objection of the CMAs. For the avoidance of doubt, the appointment of replacement nominees shall be subject to the terms of Section 3.09 below.

3.3   TTUSDS Voting. The Transaction Parties shall ensure that each Security Director is entitled to cast one (1) vote on each matter presented to the TTUSDS Board and any committee thereof, and that all decisions of the TTUSDS Board and any committee thereof require the affirmative vote of: a majority of the directors in office.

3.4   TTUSDS Quorum. TTUSDS shall ensure that a minimum of two (2) Security Directors, which must include the chair of the Security Committee, are required to be present in order to establish a quorum at any meeting of, or for any action by, the TTUSDS Board or any committee thereof. TTUSDS shall ensure that neither the TTUSDS Board nor any committee thereof convenes or takes any action in the absence of a quorum. TTUSDS shall further ensure that, in the event that the chair of the Security Committee is vacant or otherwise unable to fulfill his or her role, or fails to attend a meeting twice without justification, the Security Directors present and voting select one of the other Security Directors to serve as acting chair of the Security Committee for the purposes of establishing quorum and breaking ties.

3.5   TTUSDS Board Attendance and Meetings. TTUSDS shall ensure that attendance at all meetings of the TTUSDS Board and any committee thereof is limited to the Security Directors, the TTUSDS general manager or equivalent, the TTUSDS General Counsel, the Corporate Secretary of the TTUSDS Board, the Security Officer, the Third-Party Monitor, and such other individuals whose attendance is approved in advance by the CMAs, and, with respect to meetings of the Security Committee, the Technology Officer.

(1)   TTUSDS shall ensure that apart from those individuals expressly permitted to attend meetings of the TTUSDS Board under this Section 3.5, any other observers or attendees at meetings of the TTUSDS Board or any committee thereof are approved in writing in advance by the CMAs. At least seven (7) days in advance of a meeting of the TTUSDS Board or any committee thereof, TTUSDS shall submit a written request to the CMAs of any individual, other than those specifically listed in this Section 3.5, who is proposed to attend the meeting and provide their title, affiliation, and the purpose of their participation.

(2)   TTUSDS shall ensure that the Security Officer and Third-Party Monitor are given advance notice of, and the opportunity to, participate in all meetings of the TTUSDS Board and any committee thereof in a non-voting observer capacity, and that the Technology Officer participates in all meetings of the Security Committee in a non-voting observer capacity.

(3)   TTUSDS, in conjunction with the Security Committee, shall submit to the Security Officer, Third-Party Monitor, and CMAs: (1) copies of all board and committee materials at least one (1) day prior to any meeting, unless the Security Committee certifies in writing that exceptional circumstances require an emergency meeting of the TTUSDS Board, and in such case TTUSDS shall submit concurrent notice to the Security Officer, Third-Party Monitor, and CMAs; and (2) copies of the complete unredacted meeting minutes no more than seven (7) days following any board or committee meeting.

3.6   Security Director Duties. The Transaction Parties shall ensure that in exercising their duties, the Security Directors owe fiduciary duties exclusively to the CMAs and TTUSDS; *provided* that the Security Directors shall discharge their duties in a manner that they reasonably believe in good faith to be, in descending order: first, in the national security interest of the United States as determined by the CMAs; and second, where not inconsistent with the national security interest of the United States, in the best interests of TTUSDS, in each case subject to this Agreement. Following their appointment as Security Directors and for so long as they serve on the TTUSDS Board, TTUSDS shall ensure that none of the Security Directors has any employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates. The terms of compensation for the Security Directors, including any benefits or stock incentive awards of any of the Transaction Parties, shall be negotiated between TikTok Inc. and the Security Director and shall be paid by TTUSDS. The terms of compensation, to include the grant of any stock incentive awards, shall be fixed for the Security Directors' terms.

3.7   Security Committee. By no later than the Operational Date, the Transaction Parties shall ensure that the TTUSDS Board forms a permanent, board-level committee composed exclusively of the Security Directors to serve as the committee with the full and sole authority to decide all matters related to data security, cybersecurity, and national security for TTUSDS (the "**Security Committee**"). The Transaction Parties shall ensure that the TTUSDS governance documents reflect the Security Committee's responsibilities and provide that such governance documents cannot be further amended to eliminate the Security Committee or modify the Security Committee's rights and responsibilities without the prior written consent of the CMAs. TTUSDS shall ensure that the presence of at least two (2) Security Directors, including the Security Director who is chair of the Security Committee, is required to establish quorum for the Security Committee and that all meetings of, and action by, the Security Committee include the Security Officer. TTUSDS shall ensure that the Security Committee:

(1)   serves as the primary liaison between the TTUSDS Board and the CMAs, provides timely responses to inquiries from the CMAs, and maintains availability, upon reasonable notice from the CMAs, for discussions with the CMAs, in each case on matters relating to TTUSDS' governance and compliance with this Agreement;

(2)   oversees the implementation of all policies, procedures, protocols, and other matters relating to the TTUSDS' compliance with this Agreement;

(3)   oversees and periodically reviews TTUSDS' activities in performance of the CFIUS Functions;

(4)   meets regularly, and at least quarterly, to perform its obligations under this Agreement; and

(5)   annually certifies TTUSDS's compliance with this Agreement to the CMAs within seven (7) days of each anniversary of the Effective Date. Such certification shall be signed by all members of the Security Committee and may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall be deemed to constitute one and the same certification.

3.8   TTUSDS Recordkeeping and Related Certifications.

(1)   TTUSDS shall ensure that the TTUSDS Board prepares and retains all preparatory materials, records, journals, and minutes of all meetings and deliberations of the TTUSDS Board and any committee thereof for inspection by the CMAs for a period of at least five (5) years.

(2)   TTUSDS shall provide to the CMAs, within seven (7) days following a meeting of the TTUSDS Board or any committee thereof:

(i)   all materials provided or used at the meeting, including board presentations and related exhibits, and final versions of any draft materials previously provided;

(ii)   copies of meeting minutes certified by a Security Director to be accurate and complete as to the topics discussed at each meeting of the TTUSDS Board and any committee thereof;

(iii)   a roster of attendees at the meeting; and

(iv)   a signed certification by a Security Director in attendance that the meeting was conducted in accordance with the obligations set forth in this Agreement.

3.9   TTUSDS Director Vacancies. TTUSDS shall notify the Security Committee, Security Officer, Third-Party Monitor, and CMAs within two (2) days of receiving notice of any Security Director's planned or actual resignation, death, disability, or other circumstance creating a vacancy on the TTUSDS Board. Within twenty-one (21) days following a vacancy, TikTok Inc. shall nominate an individual to fill such vacancy consistent with the initial appointment process under Section 3.2.

3.10   TTUSDS Director Removal. The Transaction Parties shall ensure that any removal or replacement of a Security Director is subject to the following processes:

(1)   The Transaction Parties shall have the right to remove any Security Directors subject to all conditions included herein. The Transaction Parties shall not remove any Security Director until all of the following conditions are met: (1) TTUSDS has notified the Security Director, the Security Committee, the Security Officer, the Third-Party Monitor, and the CMAs at least twenty (20) days prior to the proposed removal date; (2) TTUSDS has provided a written justification to the CMAs for the removal with the notice provided at least twenty (20) days prior to the proposed removal date; (3) the CMAs have provided a written non-objection to the removal; and (4) a replacement has been nominated consistent with the initial appointment process under Section 3.2.

(2)   The Transaction Parties shall ensure that, should the CMAs provide written notice setting forth their determination (including a written justification for the removal), in their sole discretion, that any director of the TTUSDS Board has, intentionally or through gross negligence, failed to meet his or her obligations or has undermined the effectiveness of this Agreement, the CMAs may direct the Transaction Parties to remove the director and the Transaction Parties shall promptly, and in any event within two (2) days, remove such director. Within twenty-one (21) days following such removal, TikTok Inc. shall nominate a replacement consistent with the initial appointment process in Section 3.2. The Transaction Parties may, in response to such direction, seek consultations with the CMAs to resolve the concerns associated with any director, which the CMAs may engage in at their discretion but any such consultation shall not toll the deadline to remove such director or nominate a replacement.

(3)   Regardless of whether there is a vacancy among the Security Director positions, the Transaction Parties may, at their discretion, provide the names of up to five (5) nominees to serve as Security Directors for consideration by the CMAs. The CMAs may notify the Transaction Parties of their provisional approval or disapproval of the nominees to be eligible to serve as Security Directors should a position become vacant. If the CMAs provide provisional approval, TikTok Inc. shall still be required to formally nominate the potential Security Director pursuant to the initial appointment process in Section 3.2.

3.11   <u>TTUSDS Governance Documents</u>. ByteDance shall submit draft copies of all governance documents of TTUSDS (e.g.*,* articles of association, bylaws, charter, and any other documents that govern TTUSDS, collectively the "**TTUSDS Governance Documents**") to the CMAs at least fourteen (14) days prior to the Operational Date and from time to time after the Operational Date at the request of the CMAs or prior to any proposed amendment thereto. The Transaction Parties shall promptly, and in any event within five (5) days following receipt of a request from the CMAs, make any change to such governance documents requested by the CMAs to incorporate the terms of this Agreement, to the CMAs' satisfaction in their sole discretion.

(1)   ByteDance shall ensure that the TTUSDS Governance Documents cover all matters within the authority of TTUSDS shareholder and the TTUSDS Board. The Transaction Parties shall ensure that the consent of the TTUSDS shareholder is not required for any decision by the TTUSDS Board or any committee thereof, however, the TTUSDS Board shall not have the authority to approve the following material corporate actions without the affirmative consent of the TTUSDS shareholder:

(i) Corporate and tax structuring and intercompany matters, including requesting TikTok Inc. make capital contributions, determining TTUSDS' annual net profits or net losses for financial accounting and tax purposes, or making profit distributions to TikTok Inc.;

(ii) Entering into, amending, modifying, renewing, terminating, or waiving any rights under any material agreement or arrangement with the TTP related to the service levels, fees, liability allocations, indemnifications, or such other matters;

(iii) Corporate policies implemented at TTUSDS establishing the term, compensation and benefits parameters for Key Management Personnel, including the general manager, head of human resources, head of technology, and head of finance, or their equivalents consistent with ByteDance's global corporate policies;

(iv) Entering into a new material line of business of TTUSDS or its subsidiaries; making any material changes to the scope of any existing lines of business, products, or services of TTUSDS or its subsidiaries; or otherwise making any material change to the purpose or scope of the business as set forth in the Governance Documents;

(v) Issuance of new equity (including convertible instruments such as options, warrants, and convertible bonds) or any rights to subscribe for any equity (including convertible instruments such as options, warrants, and convertible bonds);

(vi) Pursuing an initial public offering or a SPAC Transaction or any other financing transaction for TTUSDS or its subsidiaries;

(vii) Entering into, amending, renewing, or terminating the following transactions, agreements, or arrangements:

(1) The sale, merger, consolidation, reorganization, dissolution, liquidation, disposal, or winding up in any manner of capital assets or businesses of TTUSDS;

(2) The merger or acquisition of the assets, equity, or business of another entity, or the issuance of equity to or a joint venture with any third party;

(3) A material investment, material licensing relationship, or other material strategic relationships in or with any third party;

(4) (x) Incurring or guaranteeing indebtedness; (y) pledging, mortgaging, leasing, or encumbering the assets of TTUSDS or any of its subsidiaries; and (z) creating or authorizing the creation of any debt security or the issuance of any liens, where the aggregate total of (x)

APP-443

through (z) is greater than five percent (5%) of the TTUSDS annual operating budget for the given year;

    (5)   Any transaction that:

        (A)   Is with a ByteDance competitor listed in Annex F or an Affiliate of a ByteDance competitor listed in Annex F;

        (B)   Results in any material negative deviation from the standards for the TikTok U.S. App and TikTok U.S. Platform set by ByteDance; *provided* that such standards are consistent with this Agreement in all respects as determined by the CMAs or the Security Committee as applicable; or

        (C)   Violates in any material respect any contracts and license agreements among the Transaction Parties and their respective subsidiaries.

    (viii)   Waiver of litigation rights, or agreement of settlement or admission of liability, fault, or noncompliance of TTUSDS or its subsidiaries;

    (ix)   Settling any litigation or other proceedings (a) for an amount exceeding [$1 million] individually or [$10 million] in the aggregate per calendar year; or (b) that involve the grant of an injunction or other equitable relief or otherwise impose any material restriction on the Transaction Parties' business and their respective subsidiaries;

    (x)   Making any material change to the accounting policies, practices, or methodologies for TTUSDS or its subsidiaries, unless otherwise required by law;

    (xi)   The filing or making of any petition under the U.S. federal bankruptcy laws or any similar law or statute of any state or any foreign country;

    (xii)   Making any changes to the existing legal rights or preferences of the shareholder interests, rights, preferences, or privileges in the ownership and governance documents of TTUSDS or any of its subsidiaries;

    (xiii)   To the extent not otherwise covered above, making any amendments to the ownership and governance documents of TTUSDS or any of its subsidiaries;

    (xiv)   The creation of any new direct or indirect subsidiary of TTUSDS or issuance or transfer of equity of any direct or indirect subsidiary of TTUSDS, in each case, other than the creation of TTUSDS itself or of a wholly owned direct or indirect subsidiary of TTUSDS;

(xv)   adoption of the overall annual budget and key performance indicators ("**KPIs**"), but only if the budget or KPIs, as applicable, do not meet the following requirements:

(1)   The budget and KPIs are within the parameters set by the TikTok, Inc. Board, and presented to and discussed with the TTUSDS Board and management; provided that the TTUSDS board confirms that the budget parameters provide sufficient funding for TTUSDS consistent with Section 2.8;

(2)   TTUSDS has provided the TikTok, Inc. Board a reasonable opportunity to review the budget and KPIs prior to TTUSDS Board approval; and

(3)   The budget's assumptions and projections are reasonable and consistent with the performance of TTUSDS as it develops.

(xvi)   Such other matters as may be added to this list with the prior written approval of the CMAs in their sole discretion.

(2)   The TTUSDS Shareholder shall be entitled to all relevant and material information necessary to make an informed decisions regarding any action or decision taken in connection with Paragraph 3.13(1) except information that the Security Committee determines in their sole discretion to be information that cannot be shared consistent with this Agreement including those matters relating to data security, cybersecurity or national security ("**Confidential Matters**").

(3)   The TTUSDS Governance Documents shall also provide that:

(i) the TTUSDS Board shall consult with the TikTok Inc. Board on determining compensation and benefits of Key Management Personnel, including the general manager, head of human resources, head of technology, and head of finance, or their equivalents. For the avoidance of doubt, the TTUSDS Board shall retain the final authority to determine the compensation and benefits of Key Management Personnel; and

(ii) the TTUSDS Board shall adopt and maintain policies that are materially consistent with corresponding policies that are produced and maintained at by the TikTok, Inc. Board of Directors to ensure consistency in operations, including, by way of example, budget planning and reporting, key performance indicators, principles on finance operations, principles on compliance and governance, principles on tax, and principles on auditing, provided such policies, as adopted by the TTUSDS Board, are consistent with this Agreement.

ARTICLE IV

GOVERNANCE OF TIKTOK INC.

4.1   TikTok Inc. Board Composition. ByteDance and TikTok Ltd. shall ensure that TikTok Inc., at least thirty (30) days prior to the Operational Date, and at all times thereafter, is governed by a board of directors (the "**TikTok Inc. Board**") of at least five (5) directors consistent with the following composition:

(1)   at least two (2) directors who are not CFIUS Restricted Persons, unless otherwise approved by the CMAs, who are employed by ByteDance or its Affiliates (the "**Inside Directors**");

(2)   at least two (2) directors who are Resident U.S. Citizens or citizens of other countries of the National Technology and Industrial Base, as defined by 10 U.S.C. § 2500 ("**NTIB**"), unless otherwise approved by the CMAs, who are not employed by ByteDance or its Affiliates (the "**Outside Directors**"); and

(3)   the TTUSDS Chair appointed pursuant to Section 3.1.

4.2   Business of TikTok Inc. By no later than the Operational Date, ByteDance and TikTok Inc. shall each ensure that the TikTok Inc. Board is responsible for the governance of the business related to the TikTok U.S. App and TikTok U.S. Platform other than those related to the CFIUS Functions, which shall be solely owned or licensed, and managed, by TTUSDS, and except as otherwise expressly provided for in this Agreement. Other than as they relate to compliance with this Agreement, the TikTok Inc. Board shall have exclusive management authority over the following matters:

(1)   Business strategy for the United States;

(2)   Coordination between the TikTok business in the United States with the rest-of-world TikTok business;

(3)   Product feature development for the United States;

(4)   Internal tool development to be used and deployed in the TikTok U.S. Platform;

(5)   TikTok U.S. User experience, including user feedback;

(6)   U.S. trust and safety;

(7)   Setting standards and measuring for the TikTok business in the United States the following: core business practices, policies, and metrics, including human resources policies, KPIs, employee morale and sentiment, and compensation policies;

(8)   Reviewing recruitment, hiring or termination, compensation, benefits, and performance of senior officers and managers for the United States to ensure consistency with the rest of the world and company policies;

(9)   Setting facilities and real estate standards for consistency with rest-of-world real estate practices;

(10)   U.S. financials and other related matters, including:

(i)   Revenue, operating expenses, and related metrics;

(ii)   Audits and reporting;

(iii)   Budgets and forecast;

(iv)   Treasury, cash, and debt;

(v)   Taxes;

(vi)   Valuation;

(11)   Legal compliance matters unrelated to this Agreement; and

(12)   such other matters that are necessary to give effect to the aforementioned listed items.

4.3   TikTok Inc. Board Voting and Quorum Requirements.

(1)   TikTok Inc. shall ensure that each director of the TikTok Inc. Board is entitled to cast one (1) vote on each matter presented to the TikTok Inc. Board and any committee thereof, and that all decisions of the TikTok Inc. Board and any committee thereof require the affirmative vote of a majority of the directors in office.

(2)   TikTok Inc. shall ensure that the presence of the TTUSDS Chair is required in order to establish a quorum at any meeting of, or for any action by, the TikTok Inc. Board or any committee thereof, unless the TTUSDS Chair has received written notice of such meetings and twice failed to attend without reasonable justification. Prior to holding any meeting of the TikTok Inc. Board without the presence of the TTUSDS Chair, TikTok Inc. shall notify the CMAs of the TTUSDS Chair's failure to attend and provide the relevant justification (if any). Whether the TTUSDS Chair's justification for his or her failure to attend constitutes "reasonable justification" for purposes of Section 4.3(2) shall be in the sole discretion of the CMAs. If the CMAs do not object in writing within ten (10) days following receipt of the TTUSDS Chair's justification for his or her failure to attend, the lack of action shall constitute a non-objection. TikTok Inc. shall ensure that neither the TikTok Inc. Board nor any committee thereof convenes or takes any action in the absence of a quorum.

(3)   TikTok Inc. shall ensure that the affirmative vote of the TTUSDS Chair is required for any decision of the TikTok Inc. Board or any committee thereof that involves any of the following with respect to TikTok Inc. or its subsidiaries, each as determined in accordance with the TTUSDS Chair's reasonable discretion and in conformance with said Director's fiduciary duties:

(i)   matters dealing with the relationship with or responsibilities of the TTP, each solely as they relate to this Agreement; and

(ii)   issues that directly impact the Transaction Parties' compliance with this Agreement.

4.4   Board Conflicts. The Transaction Parties shall ensure the business and affairs of TikTok Inc. and TTUSDS are managed, and all corporate powers are exercised by or under the direction of, the TikTok Inc. Board and TTUSDS Board, respectively. If during a meeting of the TikTok Inc. Board, the TTUSDS Chair objects to a topic of discussion, the matter shall be tabled until the Security Committee can convene to determine whether the matter appropriately falls within the scope of Section 2.4 or 4.2.

4.5   TTUSDS Chair Duties. ByteDance, TikTok Ltd., and TikTok Inc. shall ensure that in exercising his or her duties, the TTUSDS Chair owes fiduciary duties exclusively to the CMAs and TikTok Inc.; *provided* that the TTUSDS Chair shall discharge his or her duties in a manner that he or she reasonably believe in good faith to be, in descending order: first, in the national security interest of the United States as determined by the CMAs; and second, where not inconsistent with the national security interest of the United States, in the best interests of TikTok Inc., in each case subject to this Agreement.

4.6   TikTok Inc. Recordkeeping. TikTok Inc. shall ensure that the TikTok Inc. Board prepares and retains all records, journals, and minutes of all meetings and deliberations of the TikTok Inc. Board and any committee thereof for a period of at least five (5) years for inspection by the CMAs.

4.7   TTUSDS Chair Vacancy and Removal.

(1)   The TTUSDS Chair shall be subject to the same vacancy and removal provisions as in his or her capacity as a Security Director of the TTUSDS Board in accordance with Section 3.10.

(2)   The TTUSDS Chair may be removed from the TikTok Inc. Board on the same terms and conditions as set forth for Security Directors in Section 3.10. In the event of a vacancy in the TTUSDS Chair position, ByteDance shall select one (1) of the remaining Security Directors of the TTUSDS Board to assume the TTUSDS Chair position on the TikTok Inc. Board, subject to prior notice to and non-objection by the CMAs.

(3)   For the avoidance of doubt, the lapse of a term limit for any TTUSDS Chair of the TikTok Inc. Board shall trigger the processes under this Section 4.7 for the replacement of such TTUSDS Chair, including the timing requirements for replacements.

4.8   <u>TTUSDS Board and TikTok Inc. Board Coordination</u>. Notwithstanding any other provision of this Agreement, the TTUSDS Board and TikTok Inc. Board shall be permitted to meet jointly to facilitate discussion of any matters not prohibited by this Agreement. Until the one-year anniversary of the Operational Date, the TTUSDS Board and TikTok Inc. Board are recommended to meet (in-person or virtually) monthly. Following the first anniversary of the Operational Date, the TTUSDS Board and TikTok Inc. Board are recommended to meet quarterly.

<div align="center">

ARTICLE V

MANAGEMENT OF TTUSDS

</div>

5.1   <u>Key Management</u>.

(1)   Within seven (7) days following the appointment of the TTUSDS Board, TTUSDS shall ensure that the TTUSDS Board nominates individuals to serve as Key Management, and concurrently shall submit to the CMAs a list of such individuals, full internal organizational charts, and any other details reasonably requested by the CMAs for the CMAs to designate, in their sole discretion, any Personnel as Key Management. If the CMAs designate any Personnel of TTUSDS as Key Management, TTUSDS shall ensure that such Personnel are subject to the nomination, appointment, removal, and replacement processes for Key Management under Sections 5.1 and 5.2. TTUSDS shall ensure that all nominees for Key Management are Resident U.S. Citizens and hold no position within ByteDance or any of its Affiliates, in both cases for the duration of his or her service as Key Management and unless otherwise approved by the CMAs.

(2)   The appointment of any individual as Key Management shall be subject to the prior non-objection of the CMAs. For each nominee, TTUSDS shall submit complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis, contact information, and any other information requested by the CMAs to ensure that the nominee can effectively perform the functions set forth in this Agreement. TTUSDS shall ensure that each nominee is available for an interview with the CMAs, at their request. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about a nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to one or more nominees, TTUSDS shall ensure that the TTUSDS Board nominates a different candidate within twenty-one (21) days following receipt of any such objection, subject to the same procedures as the initial nomination.

(3)   TTUSDS shall ensure that the TTUSDS Board appoints each individual to serve as Key Management within three (3) days following the designation by or non-objection of the CMAs. TTUSDS shall ensure that each of the Key Management maintains his or her primary work location at a TTUSDS office location in the United States, that Key Management

are the senior officers with authority over the TikTok U.S. App and TikTok U.S. Platform in the United States, and that neither Key Management nor their subordinates report to any Personnel of ByteDance or its Affiliates.

5.2   Removal of Key Management. TTUSDS shall submit prior written notice to the CMAs before removing, replacing, or appointing any Key Management and shall not effect any such change in the event that the CMAs object in writing within fourteen (14) days following such notice; *provided, however*, that TTUSDS may immediately remove any Key Management for cause, subject to compliance with applicable law and the governance documents of TTUSDS, in which case TTUSDS shall notify the CMAs within one (1) day of such removal with an explanation of the cause. TTUSDS shall not remove any Key Management for his or her actual or attempted efforts to ensure compliance with this Agreement. TTUSDS shall ensure that the replacement and appointment of any Key Management are subject to the same process as the initial nomination and appointment process under Section 5.1.

5.3   Hiring Protocols.

(1)   Existing ByteDance Personnel. The Transaction Parties shall notify the CMAs of any ByteDance or Affiliate Personnel, including a description of their job responsibilities, who (a) are not Resident U.S. Citizens and whose employment will be transferred from ByteDance or any of its Affiliates to TTUSDS, or (b) who may have Access to Protected Data under the Limited Access Protocol, no less than thirty (30) days prior to any such Personnel beginning to work for or support TTUSDS or having Access to Protected Data under the Limited Access Protocol, as relevant. The CMAs may, within twenty-one (21) days following receipt of such notification, object in writing to such Personnel, in which event TTUSDS shall not employ, independently engage the services of, or accept the transfer of employment contracts for such Personnel. For the avoidance of doubt, this provision does not apply to Key Management whose appointment, removal, and replacement shall follow the processes under Sections 5.1 and 5.2.

(2)   Newly Hired Personnel. Within thirty (30) days following the Operational Date, TTUSDS shall develop and implement hiring protocols for onboarding newly hired Personnel (i.e., Personnel other than those originally transferred to or hired by TTUSDS as of the Operational Date) to TTUSDS. TTUSDS shall ensure that the hiring protocols provide for the vetting of whether the prospective Personnel is a CFIUS Restricted Person or has any current or prior employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates for a period of one (1) year prior to his or her potential employment or support date. In the event that such a current or prior relationship exists, TTUSDS shall obtain the CMAs' prior written consent prior to hiring, onboarding, or granting or facilitating Physical Access to facilities or Logical Access to IT systems to such prospective Personnel. For the avoidance of doubt, this provision does not apply to Key Management whose appointment, removal, and replacement shall follow the processes under Sections 5.1 and 5.2.

(3)   Reporting Lines. TTUSDS shall ensure that any Personnel transferred from ByteDance or any of its Affiliates to TTUSDS report solely to Key Management (or other

designated Personnel of TTUSDS) and do not report to any Personnel of ByteDance or its Affiliates, consistent with Section 5.1(3).

        (4)   <u>Post-Separation</u>. ByteDance shall not employ, independently engage the services of, or accept the transfer of employment contracts for any current or former employees of TTUSDS (including Key Management) for a period of one (1) year following the employee's separation from TTUSDS without the prior written consent of the CMAs. ByteDance shall ensure that none of its Affiliates, after conducting due diligence, knowingly employs, independently engages the services of, or accepts the transfer of employment contracts for any current or former employees of TTUSDS (including Key Management) for a period of one (1) year following the employee's separation from TTUSDS without the prior written consent of the CMAs except as approved in the Hiring Protocols.

        (5)   <u>TTP Hiring</u>.

        TTUSDS shall ensure that the MSA requires the TTP to implement hiring protocols consistent with Subsection 5.4(2) for any prospective Personnel of the TTP who will perform services under the MSA, and TTUSDS shall enforce such requirement of the MSA against the TTP.

        5.4   <u>Content Advisory Council</u>. Within sixty (60) days following the Operational Date, TTUSDS shall establish and maintain an external council of at least three (3) leading experts with experience in social media platforms, content moderation, free speech, or foreign influence who are Resident U.S. Citizens to advise TTUSDS on the Content Promotion and Filtering, Trust and Safety Moderation, and other content moderation policies for the TikTok U.S. App and TikTok U.S. Platform that are relevant to Trust and Safety Moderation (the "**Content Advisory Council**"). For the avoidance of doubt, the Content Advisory Council's role with respect to Content Promotion and Filtering, Trust and Safety Moderation, and other content moderation practices shall be advisory, not operational, and members of the current Content Advisory Council (established in March 2020) may serve on the Content Advisory Council under this Section 5.5. TTUSDS shall submit the name and a *curriculum vitae* or similar professional synopsis to the Third-Party Monitor and CMAs for each member of the Content Advisory Council, initially and upon any change to its composition. TTUSDS shall ensure that, at the Content Advisory Council's or CMAs' request, or at its own discretion, the Third-Party Monitor reviews human exclusions of content to ensure actions were taken consistent with Trust and Safety Moderation guidelines and delivers such reports to the Content Advisory Council upon completion. TTUSDS shall ensure that the Content Advisory Council may, as needed in its discretion, periodically engage with the Third-Party Monitor and CMAs about trends in foreign influence, propaganda, censorship, disinformation, and similar topics.

        5.5   <u>Communications Between Personnel of TTUSDS, ByteDance, and ByteDance Affiliates</u>. Notwithstanding any other provision of this Agreement, communications between TTUSDS Personnel and Personnel of ByteDance or its Affiliates shall be permitted. Electronic communications between TTUSDS Personnel, on the one hand, and Personnel of ByteDance or its Affiliates, on the other hand, shall be logged for auditing purposes.

ARTICLE VI

BYTEDANCE POC, COMPLIANCE OFFICER, AND SECURITY OFFICER

6.1   Point of Contact. ByteDance shall at all times maintain a point of contact for the Third-Party Monitor and CMAs regarding ByteDance's compliance with this Agreement (the "**ByteDance POC**"). ByteDance shall notify the CMAs of the identity of the ByteDance POC within fourteen (14) days following the Effective Date, and within three (3) days following any change in the ByteDance POC.

6.2   Compliance Officer. TikTok Inc. shall at all times employ a compliance officer (the "**Compliance Officer**") who meets the qualifications set forth in Section 6.4, serves as the senior liaison between TikTok Inc. and the Third-Party Monitor and CMAs, and is responsible for overseeing compliance with this Agreement on behalf of TikTok Inc.

6.3   Security Officer. TTUSDS shall at all times employ a security officer (the "**Security Officer**") who meets the qualifications set forth in Section 6.4, serves as the senior liaison between TTUSDS and the Third-Party Monitor and CMAs, and is responsible for overseeing compliance with this Agreement on behalf of TTUSDS. TTUSDS shall ensure that the Security Officer reports directly and exclusively to the Security Committee.

6.4   Qualifications. TikTok Inc., with respect to the Compliance Officer, and TTUSDS, with respect to the Security Officer, shall ensure that the Compliance Officer and Security Officer:

(1)   are Resident Sole U.S. Citizens who have, or are eligible for, a U.S. personnel security clearance;

(2)   are qualified employees of TikTok Inc. or TTUSDS, respectively;

(3)   have sufficient and appropriate senior-level authority and resources within TikTok Inc. or TTUSDS, respectively, and the necessary technical skills and experience to ensure compliance with this Agreement and to fulfill all other obligations of the position;

(4)   have no current or prior contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates; *provided* that the initial Compliance Officer and Security Officer may be individuals who were previously employed in the United States by TikTok Inc. or ByteDance, Inc. as of the Effective Date and, in the case of the Security Officer, who will be transferred to TTUSDS by no later than the Operational Date; and

(5)   have Physical Access and Logical Access to all of the facilities, systems, records, and meetings of TikTok Inc. or TTUSDS, respectively, that in the sole discretion of the Third-Party Monitor and CMAs, are necessary to ensure compliance with this Agreement.

APP-452

The Compliance Officer and Security Officer may hold other titles and responsibilities at TikTok Inc. and TTUSDS, respectively; *provided* that such other responsibilities do not prevent the officer from performing his or her obligations in connection with the Agreement.

6.5   Nomination and Appointment. The appointment of the Compliance Officer and Security Officer shall be subject to the prior non-objection of the CMAs. Within fourteen (14) days following the Effective Date, the Transaction Parties shall nominate an initial Compliance Officer and initial Security Officer (in the case of the Security Officer, to be transferred to TTUSDS as of the Operational Date) and submit complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis, contact information, and any other information requested by the CMAs to assess whether the individual can effectively perform the obligations of the Compliance Officer or Security Officer, as applicable, under this Agreement. If the CMAs do not object in writing within twenty-one (21) days following receipt of all necessary information about the nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object, the Transaction Parties shall nominate a different candidate within seven (7) days following receipt of any such objection, subject to the same procedures as the initial nomination. TikTok Inc. and TTUSDS, respectively, shall appoint the Compliance Officer and the Security Officer within three (3) days following non-objection by the CMAs.

6.6   Removal and Replacement.

(1)   Neither TikTok Inc. nor TTUSDS shall remove any Compliance Officer or Security Officer without the prior non-objection of the CMAs. TikTok Inc. and TTUSDS, respectively, shall notify the CMAs at least fourteen (14) days before the proposed removal of a Compliance Officer or Security Officer unless such removal is for cause, and such removal shall only be proposed in conjunction with the nomination of a new candidate for the position, subject to the same procedures as the initial nomination. For the avoidance of doubt, such cause must consist of willful misconduct, gross negligence, reckless disregard, violation of applicable law, violation of company policy, or failure of the individual to perform his or her job duties. At no time shall TikTok Inc. or TTUSDS remove, penalize, or negatively change the terms of employment, including compensation and benefits, of the Compliance Officer or Security Officer for such officer's actual or attempted efforts to comply with or ensure compliance with this Agreement.

(2)   Should the CMAs, in their sole discretion, determine that the Compliance Officer or Security Officer has failed to meet his or her respective obligations or has otherwise undermined the effectiveness of this Agreement, the CMAs may direct TikTok Inc. or TTUSDS, respectively, to remove the Compliance Officer or Security Officer, and TikTok Inc. or TTUSDS, respectively, shall promptly, and in any event within two (2) days, remove such officer.

(3)   In the event of any vacancy in the Compliance Officer or Security Officer position, TikTok Inc. or TTUSDS, respectively, shall notify the CMAs within one (1) day and, within fourteen (14) days following such vacancy occurring, nominate a replacement Compliance Officer or Security Officer, subject to the same procedures as the initial nomination.

During any vacancy of the Security Officer position, TTUSDS shall ensure that the chairman of the Security Committee fulfills the obligations of the Security Officer.

6.7   Communication with the Third-Party Monitor and CMAs. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, provide timely responses to inquiries from the Third-Party Monitor and CMAs about TikTok Inc.'s and TTUSDS's respective compliance with this Agreement. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, maintain availability for discussions with the Third-Party Monitor and CMAs on matters relating to compliance with this Agreement.

6.8   Reporting of Violations. TikTok Inc. and TTUSDS shall ensure that the Compliance Officer and Security Officer, respectively, report any actual or potential violation of this Agreement to the Third-Party Monitor and CMAs as soon as practicable, but in any event within one (1) day of learning of the actual or potential violation.

6.9   Costs. TikTok Inc. shall be responsible for all costs associated with the Compliance Officer and TTUSDS shall be responsible for all costs associated with the Security Officer.

6.10   Applicability Rule. Prior to the Operational Date, and unless otherwise specified in this Article VI, ByteDance and TikTok Inc. shall fulfill the requirements of this Article VI. Following the Operational Date, TTUSDS shall assume exclusive responsibility for the Security Officer.

ARTICLE VII

LAWFUL U.S. PROCESS

7.1   Lawful U.S. Process. TikTok Inc. and TTUSDS acknowledge their respective obligations to comply with valid Lawful U.S. Process. Without limiting such obligations, TikTok Inc. and TTUSDS agree that TTUSDS shall be principally responsible for complying with Lawful U.S. Process requests, whether directed at TikTok Inc. or TTUSDS, unless otherwise provided for in the Limited Access Protocol pursuant to Section 11.9. To this end, TTUSDS shall maintain policies relating to Lawful U.S. Process-related activities, regarding the security measures for handling, retaining, managing, and deleting information about Lawful U.S. Process-related activities. Those policies shall be subject to review by the Security Officer and approval by the Security Committee. No later than ninety (90) days after the Operational Date, TTUSDS shall deliver the Security Committee-approved policies relating to Lawful U.S. Process-related activities to the CMAs for their review and written approval. Subsequent changes to such policies also will be subject to the CMAs' written approval, excluding non-substantive revisions (e.g., typographical corrections).

<u>**ARTICLE VIII**</u>

<u>**TRUSTED TECHNOLOGY PROVIDER**</u>

8.1   <u>Independence</u>. At all times during any TTP's provision of services in connection with this Agreement, the Transaction Parties shall not have, and shall ensure that their respective Affiliates do not have, any financial or voting interest in, or otherwise possess an ability to Control, the TTP or its provision of services in connection with this Agreement, except to the extent necessary to enforce and ensure compliance with the MSA executed following the non-objection of the CMAs. The Transaction Parties shall treat the TTP as an arm's-length commercial vendor, and none of the Transaction Parties shall engage in any transaction following the Effective Date through which the TTP gains an equity interest in, or any governance rights with respect to, any of the Transaction Parties.

8.2   <u>Master Services Agreement</u>.

(1)   Within forty five (45) days following the Effective Date, the Transaction Parties shall, in coordination with the TTP, submit an initial draft MSA to the CMAs. The MSA, including any amendments thereto, shall be subject to the prior non-objection of the CMAs. The Transaction Parties, in coordination with the TTP, shall subsequently submit a draft of the MSA, and any amendments thereto, to the CMAs, and resolve any concerns raised by the CMAs to the CMAs' satisfaction prior to the execution of the MSA or any amendment thereto. If the CMAs do not object in writing within forty-five (45) days following receipt of a draft MSA or amendment, the lack of action shall constitute a non-objection. The Transaction Parties shall execute the MSA or any amendment thereto within three (3) days following the non-objection of the CMAs (if executed prior to the Operational Date, the Transaction Party shall ensure that TTUSDS joins as a party to the MSA by no later than the Operational Date). The Transaction Parties shall submit a copy of the final MSA and any amendment thereto to the CMAs within three (3) days following execution. In the event that Oracle (or a successor TTP) is replaced as the TTP, the Transaction Parties shall execute an MSA with the replacement TTP following the non-objection of the CMAS to the replacement TTP under Section 8.2(6), in accordance with the procedures and requirements for the initial MSA.

(2)   The Transaction Parties shall ensure that the MSA incorporates all of the provisions applicable to the TTP, Protected Data, Source Code and Related Files, Recommendation Engine, and the TikTok U.S. App and TikTok U.S. Platform under this Agreement, and further incorporates the obligations of the Transaction Parties under this Agreement to ensure that the TTP takes the actions specified in this Agreement and that TTUSDS fully cooperates with the TTP to ensure that the TTP can take such actions as specified in this Agreement, in all cases to the CMAs' satisfaction in their sole discretion.

(3)   The Transaction Parties shall ensure the TTP receives all submissions of findings arising from the public bug bounty program for the TikTok U.S. App.

(4)   The Transaction Parties shall ensure that the MSA sets forth specific commitments by TTUSDS and Oracle (or a successor TTP), including submitting to oversight

and auditing by the CMAs and third parties designated under this Agreement of services performed under the MSA. The Transaction Parties shall ensure the MSA grants the TTP the right, in its sole discretion, to seek the views of the Third-Party Monitor and CMAs in the event of any disagreement between the Transaction Parties and the TTP regarding the security of Protected Data and Source Code and Related Files.

(5)   The Transaction Parties shall amend the MSA upon written direction from the CMAs, in their sole discretion; *provided* that any amendments to the MSA initiated by the CMAs shall be for purposes of ensuring compliance with this Agreement and after consultation with the Transaction Parties, the TTP, and the Third-Party Monitor.

(6)   The Transaction Parties may, solely based on evidence that the TTP has failed to comply with the material terms of the MSA and with notice to the CMAs regarding the provision(s) breached and supporting evidence, request that the CMAs permit the Transaction Parties to remove the TTP for cause. The Transaction Parties shall not remove the TTP without the prior written consent of the CMAs. The CMAs, in their sole discretion, may require the Transaction Parties to remove and replace the TTP. The Transaction Parties shall ensure that the MSA provides for a process to effectively transition responsibilities in connection with this Agreement to a new TTP in the event of a removal or replacement. Within thirty (30) days following any vacancy in the TTP position, the Transaction Parties shall submit for the prior non-objection of the CMAs the name and any additional information requested by the CMAs of a proposed vendor to serve as the TTP. If the CMAs object, the Transaction Parties shall not engage the vendor and shall submit another proposed vendor to the CMAs within thirty (30) days following receipt of the CMAs' objection. If the CMAs do not object within thirty (30) days following receipt of all necessary information regarding a proposed replacement TTP, the lack of action shall constitute a non-objection.

(7)   The Transaction Parties shall provide sufficient financial resources, consistent with industry-standard rates for comparable services and determined in coordination with the TTP, to enable the TTP to fully perform the responsibilities designated to the TTP in connection with this Agreement and under the MSA. The Transaction Parties shall ensure that the MSA requires the TTP to promptly notify the CMAs if the TTP believes, in its sole discretion that it lacks sufficient funding or related resources under the MSA to adequately conduct the tasks required of it under the MSA and in connection with this Agreement. The Transaction Parties shall provide semi-annual updates to the Third-Party Monitor and CMAs regarding the budgeting and funding of the TTP under the MSA and in connection with this Agreement.

8.3   Rule of Construction. Any provision of this Agreement that requires any Transaction Party, individually or collectively, to ensure that the TTP takes a specified action shall be deemed to require the applicable Transaction Party to enforce, contractually through the MSA, the TTP's fulfillment of and compliance with its obligations in connection with this Agreement.

8.4   TikTok U.S. Platform Deployment. By no later than the Operational Date, the Transaction Parties shall, in coordination with the TTP, take all steps necessary to facilitate TTUSDS's initial deployment of the TikTok U.S. Platform in the TTP's secure cloud

infrastructure in the United States, which shall be logically separate from the DTC, and thereafter the Transaction Parties shall ensure that TTUSDS continues to maintain and operate the TikTok U.S. Platform exclusively in the TTP's secure cloud infrastructure in the United States, except as otherwise provided in this Agreement (including with respect to CDNs). The Transaction Parties shall ensure that TTUSDS's deployment of the TikTok U.S. Platform includes the creation of secure testing, build, integration, and deployment environments for the TikTok U.S. App and TikTok U.S. Platform that are permissioned and auditable. The Transaction Parties shall ensure the TTP implements processes and controls to monitor these environments to ensure compliance with this Agreement related to Source Code and Related Files and Logical Access to Protected Data.

8.5   Content Delivery Networks. TTUSDS shall not be required to maintain and operate CDNs solely within the TTP's secure cloud infrastructure; *provided* that TTUSDS shall maintain, operate, and contract for any CDN that is not within the TTP's secure cloud infrastructure in accordance with the following requirements:

(1)   Commercial CDNs: TTUSDS shall ensure that the use of any third-party CDN providers for the TikTok U.S. Platform complies with the vendor approval requirements, including the Vendor Program Policy pursuant to Article XIII of this Agreement.

(i)   TTUSDS shall ensure that all such CDN servers utilized for the delivery of content in the United States reside exclusively in the United States.

(ii)   TTUSDS shall consult with the TTP and Third-Party Monitor on configuration changes related to a CDN. All such changes shall be logged in auditable fashion, with the logs made available to the Third-Party Monitor, the Third-Party Auditor, and the CMAs. TTUSDS shall involve the TTP in any discussions or work with the third-party CDN provider related to such configuration changes.

(iii)   TTUSDS shall ensure that the TTP has the ability to monitor and audit configuration changes related to CDNs through a gateway in the TTP's secure cloud infrastructure for Access to the CDN network elements or the built-in capability provided by the commercial CDN. TTUSDS shall ensure that the gateway or built-in capability of the commercial CDN includes an alert system that notifies both TTUSDS and the TTP of any change of origin settings or that otherwise results in unexpected traffic routing patterns.

(2)   Proprietary CDNs.

(i)   All Source Code and Related Files for any proprietary CDN servers maintained by TTUSDS shall be subject to the applicable software assurance requirements of Article IX, including review and testing by the TTP in parallel with deployment of Executable Code.

(ii)   TTUSDS shall work with the TTP to develop technical means that enable (a) the TTP to monitor the interaction of the servers with the other elements of the

TikTok U.S. Platform and systems operated by or on behalf of ByteDance serving non-TikTok U.S. Users, and (b) the TTP to block any such interactions that are unexpected or unauthorized and report, within one (1) day of discovery and validation, any such interactions to the Third-Party Monitor and CMAs.

(iii)   Any proprietary CDN servers maintained by TTUSDS shall not Access any Protected Data other than IP addresses, which TTUSDS shall ensure are masked when stored on the CDN server, unless TTUSDS requests, and the CMAs approve, Access by the CDN to any other Protected Data.

(iv)   On an annual basis, TTUSDS shall, with input from the TTP and Third-Party Monitor, reevaluate and report to the CMAs regarding the feasibility of third-party vendors adequately supporting services covered by proprietary CDNs. When TTUSDS concludes that third-party vendors can adequately support the services provided by proprietary CDNs consistent with industry-standard rates for comparable services, TTUSDS shall transition those services to a third-party vendor on a timeline established in consultation with the TTP, Third-Party Monitor, and CMAs.

(3)   For the avoidance of doubt, neither ByteDance nor any of its Affiliates shall have Access to the CDNs supporting the TikTok U.S. Platform.

8.6   Diagrams. By no later than thirty (30) days prior to the Operational Date, and thereafter within fourteen (14) days following a request from the CMAs, the Transaction Parties shall submit, and shall ensure the TTP submits, respectively as applicable to their individual obligations or collectively as appropriate, Architecture Diagrams, Data Flow Diagrams, Existing Network Diagrams, and Source Code Review Diagrams for the TikTok U.S. Platform to the Third-Party Monitor and CMAs. The Transaction Parties shall promptly respond, and shall ensure the TTP promptly responds, to inquiries from the Third-Party Monitor and CMAs for further or clarifying information regarding any submission of Architecture Diagrams, Data Flow Diagrams, Existing Network Diagrams, and Source Code Review Diagrams.

ARTICLE IX

DEDICATED TRANSPARENCY CENTER AND SOURCE CODE SECURITY

9.1   DTC Locations and Protocols. The Transaction Parties shall mutually develop with the TTP the locations and Physical Access and Logical Access procedures of the DTC, as well as the security requirements, infrastructure, technical and architectural parameters, and equipment to be used within the DTC (together, the "**DTC Operating Protocols**"). The Transaction Parties shall ensure that the DTC is located at all times in the United States; *except that* supporting DTCs may be located in the United Kingdom, Australia, New Zealand, and Canada (the "**DTC Approved Countries**"). The Transaction Parties shall at all times comply with the DTC Operating Protocols (as amended from time to time, at the request of the Transaction Parties or TTP, or at the direction of the CMAs). The Transaction Parties shall not amend the DTC Operating Protocols without the prior written consent of the TTP.

(1)   The DTC Operating Protocols and any amendments thereto shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit the DTC Operating Protocols to the CMAs within seven (7) days following the Effective Date. The Transaction Parties shall submit written confirmation to the CMAs of the TTP's agreement to the initial DTC Operating Protocols and any amendment thereto. If the CMAs do not object in writing within fourteen (14) days following receipt of the DTC Operating Protocols or any amendment thereto, the lack of action shall constitute a non-objection. If the CMAs object, the Transaction Parties shall fully resolve the CMAs' concerns to the satisfaction of the CMAs in their sole discretion before implementing the DTC Operating Protocols or any amendment thereto. The Transaction Parties shall adopt and implement the DTC Operating Protocols with the TTP following the non-objection of the CMAs and by no later than the Operational Date.

(2)   The Transaction Parties shall not, and shall ensure that their respective Affiliates do not, Access or use the DTC except in accordance with the DTC Operating Protocols.

9.2   Provision of Source Code and Related Files via the DTC.

(1)   ByteDance shall provide, and shall ensure that its Affiliates provide, all current and future Source Code and Related Files to the TTP and the Source Code Inspector via the DTC for the purposes of software assurance and secure deployment of the TikTok U.S. App and TikTok U.S. Platform, as well as the performance of all related services under the MSA. ByteDance shall initially provide, and shall ensure that its Affiliates provide, all current Source Code and Related Files to the TTP via the DTC by no later than the Operational Date and on an ongoing basis thereafter. The transfer of Source Code and Related Files to the TTP via the DTC shall not be deemed to transfer any title that ByteDance or any of its Affiliates has in the Source Code and Related Files.

(2)   In connection with its provision of all current and future Source Code and Related Files to the TTP via the DTC, ByteDance shall produce a software bill of materials (the "**SBOM**") or its equivalent, that inventories, for each version of the Source Code and Related Files, all components and their origin, including sufficient data for the TTP to verify each component and to cross-reference with known vulnerabilities. The Transaction Parties shall ensure the TTP, through signature verification (to the extent possible), verifies that the software versions and other components identified in the SBOM or its equivalent matches the Source Code and Related Files where source code is available (e.g., third-party libraries), and any third-party software, including for any build artifacts that are incorporated into the TikTok U.S. App or the TikTok U.S. Platform by reference to software repositories. The Transaction Parties shall also ensure the TTP verifies, to the extent that it determines necessary and feasible, third-party software where the source code is not available (e.g., commercial-off-the-shelf software and open source tools).

(3)   The Transaction Parties shall designate Personnel who are based in the United States, Australia, New Zealand, Canada, and the United Kingdom, unless otherwise approved in writing by the CMAs, as primary points of contact with the TTP and the CMAs for requirements related to the DTC and Source Code and Related Files.

9.3   <u>DTC Access</u>.

(1)   ByteDance shall not withhold, and shall ensure that none of its Affiliates withhold, Physical Access to the DTC without just cause (e.g., for the protection of its intellectual property) and on terms consistent with the MSA and this Agreement. ByteDance shall ensure that all Persons designated in writing by the CMAs, in their sole discretion, have Access to the DTC. Any Person designated by the CMAs pursuant to this section shall treat all information such Person observes or has Access to as confidential information consistent with 31 C.F.R. § 800.802.

(2)   ByteDance shall ensure that any confidentiality requirements for Access to the DTC do not impede the ability of the Third-Party Monitor or the CMAs to conduct monitoring pursuant to this Agreement.

(3)   ByteDance shall grant, and shall ensure that its Affiliates grant, all Personnel of TTUSDS, the TTP, the Source Code Inspector, and the Third-Party Monitor Physical Access to the DTC, consistent with the DTC Operating Protocols. ByteDance shall ensure that such Personnel have a constant and consistent right and ability to have Physical Access to the DTC. ByteDance shall not take, and shall ensure that none of its Affiliates take, any action to delay or prevent Physical Access to the DTC by Personnel of TTUSDS, the TTP, the Source Code Inspector, or the Third-Party Monitor. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.3(3) to the Third-Party Monitor and CMAs.

(4)   ByteDance shall grant, and shall ensure that its Affiliates grant, Personnel of TTUSDS and the TTP full Logical Access to, and the practical ability to review and inspect, all Source Code and Related Files in the DTC, consistent with the licensing terms under Section 2.5 (including any confidentiality terms) and this Agreement, without any interference by ByteDance. ByteDance may maintain monitoring within the DTC to the extent necessary to protect its intellectual property; *provided* that such monitoring shall not impede or compromise the integrity of the TTP's confidential inspection of Source Code and Related Files. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.3(4) to the Third-Party Monitor and CMAs.

9.4   <u>Source Code and Related Files Location</u>. ByteDance may require in the DTC Operating Protocols that the TTP Personnel shall not review or inspect Source Code and Related Files other than via the DTC and that the Source Code and Related Files be used solely for the purposes required under this Agreement. ByteDance shall ensure that at least one (1) location of the DTC is within the facilities of the TTP. TTUSDS shall ensure the TTP maintains Logical Access to Source Code and Related Files via the DTC, consistent with the DTC Operating Protocols, to conduct automated and manual review of Source Code and Related Files.

9.5   <u>Software Assurance Process</u>. As part of the software assurance process, the Transaction Parties shall ensure that the Source Code and Related Files and Executable Code do not include Malicious Code.

9.6   <u>Vulnerability Reporting</u>. TTUSDS shall report promptly, and shall ensure the TTP reports promptly, via a format mutually acceptable to the CMAs and TTUSDS, and in any event within one (1) business day of discovery and validation, any findings of zero day vulnerabilities designated by the TTP as at least high severity or equivalent (following consultation with TTUSDS and based on recognized criteria such as the Common Vulnerability Scoring System and the TTP's judgment regarding whether the vulnerabilities are exploitable) or any instance of Malicious Code in the Source Code and Related Files or Executable Code to ByteDance, the Third-Party Monitor, and the CMAs, subject to the following:

(1)   In the event that the TTP discovers what it believes to be, in its sole discretion, the presence of Malicious Code in the Source Code and Related Files or Executable Code, TTUSDS shall ensure the TTP submits the written report directly to the CMAs and Third-Party Monitor prior to notifying ByteDance, and, at the direction of the CMAs, provide a copy to ByteDance soon thereafter in which the TTP may redact information, in its sole discretion or at the direction of the CMAs.

(2)   The Transaction Parties shall not disclose, and shall ensure the TTP does not disclose, to the public any findings of zero days, vulnerabilities, or Malicious Code in the Source Code and Related Files or Executable Code discovered by the TTP or the Transaction Parties unless:

(i)   they are required to do so by applicable law or regulation or in relation to a judicial or administrative proceeding;

(ii)   there is no disagreement among ByteDance, TTUSDS, and the TTP regarding the findings; or

(iii)   in the event that there is such a disagreement among ByteDance, TTUSDS, and the TTP, TTUSDS or the TTP determines, after consultation with the Security Committee, that disclosure is merited given industry practices on responsible disclosure, such as the International Organization for Standardization ("**ISO**") 29147 Standard.

(3)   TTUSDS shall ensure that the timing and contents of any public disclosure pursuant to this Section are consistent with industry practices on responsible disclosure, such as the ISO 29147 standard, to ensure that the zero day, vulnerability, or Malicious Code is remediated or otherwise patched prior to disclosure, and that the disclosure does not lead to exploitation of the zero day, vulnerability, or Malicious Code.

(4)   TTUSDS shall ensure that any public disclosure of a zero day, vulnerability, or Malicious Code is first notified to the other Transaction Parties, the TTP, the Security Committee, the Third-Party Monitor, and the CMAs. The Transaction Parties shall not disclose, shall ensure the TTP and the Third-Party Monitor do not disclose, and shall ensure that the Security Committee does not disclose, any zero day, vulnerability, or Malicious Code that is so pre-notified to them, until after it is made public by TTUSDS or the TTP consistent with this

Section 9.6(4), and the Transaction Parties shall ensure that any such disclosure is limited to the content made public by TTUSDS or the TTP.

9.7   Source Code and Related Files Review Process. Upon receiving Source Code and Related Files via the DTC, initially and for any subsequent change, TTUSDS shall ensure the TTP deploys, immediately and on an ongoing basis, a team of engineers to examine all aspects of the Source Code and Related Files using all tools required in the TTP's sole discretion, including both automated tools and human inspection, to assess the presence of any zero days, vulnerabilities, or Malicious Code, that could affect the confidentiality, integrity, or availability of the TikTok U.S. App, TikTok U.S. Platform, or Protected Data. The Transaction Parties shall permit, and shall ensure that their respective Affiliates permit, use by the TTP of all tools necessary to perform the obligations in connection with this Agreement.

9.8   TikTok U.S. App Mobile Security Measures. Within sixty (60) days following the Operational Date, or as otherwise extended by the CMAs, TTUSDS shall submit to the CMAs protocols developed with the TTP that ensure the TTP creates protections to ensure that the TikTok U.S. App cannot Access or transmit Protected Data in an unauthorized manner or exploit the mobile devices of TikTok U.S. Users (the "**Security Protocols**"). TTUSDS shall ensure that the protections are effective no later than one hundred and twenty (120) days following the Operational Date, unless otherwise extended by the CMAs. TTUSDS shall ensure the TTP agrees, in writing, with the extent and scope of the security measures in the initial protocols for each of the different apps comprising the TikTok U.S. App. For the iOS and Android mobile apps, the initial protocols shall include measures such as: activation logic to enable the mobile security measures for all TikTok U.S. Users; rules-based interceptors to analyze and, if necessary, block data flows; auditing and logging of application behavior to alert the TTP of any issues; and configuration services to enable the TTP to adjust the mobile sandbox as needed in its sole discretion. Within seven (7) days following the implementation of the Security Protocols, ByteDance shall ensure that all TikTok U.S. Users must download or update to the version of the TikTok U.S. App that includes the protections of the Security Protocols (e.g., that includes the mobile security measures to use the TikTok U.S. App). TTUSDS shall ensure the TTP submits monthly reports to the Third-Party Monitor and CMAs on its progress implementing the mobile security measures. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with the Security Protocols to the Third-Party Monitor and CMAs.

9.9   Initial Source Code and Related Files Inspection.

(1)   Within one hundred and eighty (180) days following the Operational Date, or as otherwise extended by the CMAs, TTUSDS shall ensure the TTP completes the initial inspection of Source Code and Related Files pursuant to Section 9.7 (the "**Initial Inspection**"), with the timing (other than the due date) and manner of the Initial Inspection determined by the TTP in its sole discretion. TTUSDS shall ensure the TTP submits to the Third-Party Monitor and CMAs no later than three (3) days following the completion of the Initial Inspection a certification of completion of the Initial Inspection, which shall include a summary of the findings of the Initial Inspection and no later than ten (10) days following the completion of the Initial Inspection a plan and timeline for any resulting remediations to the Source Code and

Related Files requested of or made by ByteDance as a result of the Initial Inspection. TTUSDS shall ensure the TTP submits monthly reports to the Third-Party Monitor and CMAs on its progress completing the Initial Inspection.

(2)   During the Initial Inspection, ByteDance and its Affiliates may continue to update the Source Code and Related Files or subsets thereof; *provided, however*, that ByteDance shall ensure that any such updates do not impede the Initial Inspection and are clearly identifiable as updates upon inspection by the TTP. Prior to the deployment of any updates to the Source Code and Related Files prior to the completion of the Initial Inspection, ByteDance shall consult with TTUSDS and the TTP regarding the impact of any such updates on the Initial Inspection and, where in the TTP's sole discretion such updates will impede the timely completion of the Initial Inspection, ByteDance shall not make, and shall ensure that none of its Affiliates make, such updates. TTUSDS shall ensure the TTP reports ByteDance's or its Affiliates' failure to refrain from updating the Source Code and Related Files as required by this Section 9.9(2) to the Third-Party Monitor and CMAs and includes any updates to the Source Code and Related Files in the Initial Inspection, with the Initial Inspection considered incomplete until all updates are evaluated.

9.10   Prohibition on Deployment without TTP Security Processes.

(1)   The Transaction Parties shall not deploy, and shall ensure that none of their respective Affiliates deploys, to the TikTok U.S. App or TikTok U.S. Platform any changes, updates, alterations, or improvements to the Source Code and Related Files that are not subject to security review and inspection by the TTP. For changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. App, the Transaction Parties shall ensure the TTP completes its inspection before such updates are deployed, and made available to TikTok U.S. Users. For changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. Platform, the Transaction Parties shall ensure the TTP conducts its inspection asynchronously in accordance with the Software Assurance Protocols but no later than thirty (30) days following deployment. The Transaction Parties shall ensure that only Source Code and Related Files for which the SBOM or its equivalent has been digitally signed by the TTP is deployed to the TikTok U.S. Platform. The Transaction Parties shall further ensure that any executable files derived from the Source Code and Related Files and deployed on the TikTok U.S. Platform are compiled exclusively within the TTP's secure cloud infrastructure. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.10(1) to the Third-Party Monitor and CMAs.

(2)   ByteDance shall address, and shall ensure that its Affiliates address, all issues with the Source Code and Related Files to the satisfaction of TTUSDS and the TTP, in their sole discretion. In the event of a disagreement between TTUSDS and the TTP regarding the security of the Source Code and Related Files, the view of the Security Committee shall prevail; *provided* that should the TTP seek the view of the CMAs in the event of a disagreement with the Security Committee, the view of the CMAs shall prevail. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 9.10(2) to the Third-Party Monitor and CMAs.

(3)   In all cases, the Transaction Parties shall ensure the TTP determines, in its sole discretion, when its security review and inspection pursuant to this Section 9.10 is complete.

(i)   If at any time there are insufficient funds or time for the TTP to fulfill its obligations, TTUSDS shall ensure the TTP immediately informs ByteDance and the Third-Party Monitor of the insufficiency. If, upon notification of a perceived funding insufficiency, the Security Committee determines unanimously that the TTP's request is inconsistent with industry-standard rates for comparable services, TTUSDS and the TTP shall resolve the disagreement consistent with the terms of the MSA and the timelines under Section 9.10(3)(ii) shall be tolled during such resolution. For the avoidance of doubt, tolling under this Section 9.10(3)(i) shall not affect the requirement that all changes, updates, alterations, or improvements to the Source Code and Related Files must undergo security review and inspection by the TTP consistent with Section 9.10(1), including the requirement that any such changes to the Source Code and Related Files for the TikTok U.S. App be reviewed and inspected prior to deployment to TikTok U.S. Users.

(ii)   ByteDance shall resolve any insufficiency of funding or time within fifteen (15) days of receipt of the notice under Section 9.10(3)(i). If such funding or timing insufficiency is not resolved within five (5) days, TTUSDS shall ensure the TTP immediately reports such insufficiency to the Third-Party Monitor and CMAs.

9.11   Source Code Inspector.

(1)   The Transaction Parties shall engage a third-party selected by TTUSDS and the TTP to serve as an independent inspector (the "**Source Code Inspector**") of the Source Code and Related Files in the DTC. The engagement of the Source Code Inspector shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit for the CMAs' review a proposed Source Code Inspector within sixty (60) days following the Operational Date. If the CMAs object, the Transaction Parties shall submit another proposed candidate for the CMAs' review within thirty (30) days following receipt of the objection. If the CMAs do not object within fourteen (14) days following receipt of all necessary information about a candidate, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. The Transaction Parties shall annually place funds in escrow to retain the Source Code Inspector. The Transaction Parties shall ensure that the CMAs are third-party beneficiaries of their agreement with the Source Code Inspector.

(2)   The Transaction Parties shall ensure that the Source Code Inspector is granted all Physical Access and Logical Access necessary to conduct a security vulnerability assessment within the DTC pursuant to protocols approved in advance by the CMAs and submits reports directly to the CMAs and Third-Party Monitor, with a copy to the Transaction Parties and the TTP, on a schedule determined by the CMAs.

(3)   The Transaction Parties shall ensure that the Source Code Inspector submits quarterly reports to the Transaction Parties, the TTP, and the Third-Party Monitor detailing any findings of concern, or if none, stating so. The Transaction Parties shall submit a

copy of any such report to the CMAs within three (3) days following a request by the CMAs. The CMAs may, in their sole discretion, change the frequency of the Source Code Inspector's reporting obligations.

(4)   The Transaction Parties, in coordination with the TTP, shall promptly address all findings of concern identified by the Source Code Inspector.

9.12   <u>Source Code Lifecycle</u>.

(1)   ByteDance shall develop the Source Code and Related Files and provide a mirror repository of it to the TTP, including the SBOM or its equivalent, via the DTC such that the TTP can at all times maintain full and simultaneous visibility into the Source Code and Related Files and any changes thereto via the DTC. Any changes, updates, alterations, or improvements to the Source Code and Related Files must: (i) for the TikTok U.S. App, be batched in logical collections according to a regular release schedule (except for time-sensitive changes, updates, alterations, or improvements); and (ii) for the TikTok U.S. App and TikTok U.S. Platform, only use build artifacts, whether proprietary or third-party build artifacts, from a repository within the TTP's secure cloud infrastructure and to be included in the SBOM or its equivalent.

(2)   The Transaction Parties shall meet regularly, and no less than quarterly, with the TTP and Third-Party Monitor to discuss planned changes, updates, alterations, or improvements to the Source Code and Related Files for the TikTok U.S. App and TikTok U.S. Platform, including new features, functionality, and other product roadmaps, and their implications for security and the TTP's assurance processes and responsibilities.

(3)   Only TTUSDS and the TTP shall compile the Source Code and Related Files. Once compiled, TTUSDS and the TTP shall generate the SBOM for the code they have respectively compiled, and the TTP shall digitally sign each such SBOM, exclusively via the DTC.

(4)   TTUSDS and the TTP shall only deploy Executable Code to the TikTok U.S. App and TikTok U.S. Platform in compliance with the security review and inspection requirements of Section 9.10 and may remove Executable Code from the DTC for that purpose.

(5)   The Transaction Parties shall ensure that the DTC affords the TTP and TTUSDS an end-to-end secure deployment system established by the TTP and TTUSDS for the deployment of the TikTok U.S. App and TikTok U.S. Platform, respectively, that implements the following operations with respect to Source Code and Related Files:

(i)   Any Source Code and Related Files shall not be deployed to the TikTok U.S. App and TikTok U.S. Platform unless it is subject to the security review and inspection protocols of the TTP pursuant to Section 9.10;

        (ii)   TTUSDS and the TTP shall have the ability to securely monitor and inspect the end-to-end Source Code and Related Files deployment lifecycle to ensure the integrity of the chain of custody; and

        (iii)   Source Code and Related Files shall not be removed from the DTC.

9.13   <u>Recommendation Engine and Content Moderation Processes</u>.

        (1)   On or before the Operational Date, TTUSDS shall provide to the Content Advisory Council, the TTP, and the Third-Party Monitor a copy of the U.S. playbook for human moderators, which shall be subject to approval by the Security Committee. Subsequently, TTUSDS shall provide an updated copy of this playbook to the Content Advisory Council and Security Committee any time changes are made to it. An updated copy shall also be provided to the Third-Party Monitor, the TTP, and the CMAs upon request.

        (2)   Within sixty (60) days following the Operational Date:

        (i)   The Transaction Parties shall ensure the TTP begins conducting periodic software inspection and testing of the Software and associated data implementing the Recommendation Engine to ensure that its machine-implemented rules and algorithms conform to the documentation provided to the TTP by TTUSDS and that the Software and data associated with Content Promotion and Filtering and Trust and Safety Moderation systems (together, "**Content Moderation Processes**") also conform to the published policies for the TikTok U.S. App. TTUSDS shall ensure that the Recommendation Engine is trained exclusively within the TTP's secure cloud infrastructure.

        (ii)   If the TTP or the Third-Party Monitor determine that the documentation and policies described in Section 9.13(1)(i) are insufficient to support the inspections and reviews described in this Section 9.13, then either the TTP or the TPM may inform TTUSDS and TTUSDS shall promptly deliver supplementary documentation. TTUSDS shall update the documentation described in this Section 9.13 from time to time as the Recommendation Engine, and Content Moderation Processes evolve.

        (iii)   The TTP and TPM shall report any findings under this Section 9.13(2) to the Security Committee on an ongoing basis, including any findings of material inconsistencies between the Recommendation Engine and the Content Moderation Processes and the related documentation and policies within one (1) day of discovery and validation. Upon receipt of a report from the TTP, the Security Committee and TPM, in consultation with the TTP and Content Advisory Council, shall evaluate and determine whether results of the inspection and testing of the source code implementing the Recommendation Engine and Content Moderation Processes are not operating in material conformance with the documentation and policies ("**Adverse Findings**"). For the avoidance of doubt, it is understood that the operation of the Recommendation Engine

and Content Moderation Processes in conformance with related documentation and policies may result in diverse content being published via the TikTok U.S. App because of the nature of the underlying machine learning technologies and not because of inconsistencies between the operation of the Software and the related documentation and policies and so Adverse Findings shall not be based solely on outcome-based evidence.

(iv)   At the request of the Security Committee, the CMAs, or the TTP, the Third-Party Auditor shall conduct an audit of the Content Moderation Processes' implementation for consistency with approved Content Moderation Processes policies and guidelines.

(v)   In the event of an Adverse Finding, ByteDance shall, in consultation with TTUSDS and the TTP, as appropriate and necessary, promptly implement any necessary changes or updates to the Software implementing the Recommendation Engine and Content Moderation Processes, as applicable, to the extent necessary to address such findings. If ByteDance is unable or unwilling to do so the CMAs shall, in consultation with TTUSDS, the Content Advisory Council, and the Security Committee, determine whether—contrary to ByteDance's conclusion—a remediation plan is feasible within a reasonable period of time.

(1)   If on the basis of the consultation required by the prior paragraph the CMAs determine:

(X) it is not feasible within a reasonable period of time for a remediation plan to be implemented; or

(Y) ByteDance, in consultation with TTUSDS and the TTP, as appropriate and necessary, fails to implement any necessary changes or updates required by the remediation plan to the Software implementing the Recommendation Engine and Content Moderation Processes, as applicable,

then the CMAs may make the Adverse Findings public following the process described in this section and after first consulting with the Security Committee regarding the content of any such public statement and providing ByteDance with the opportunity to review and provide comments on the content of the statement at least two (2) days prior to release of the public statement.

9.14   Further Testing of Source Code and Related Files. At the request of the CMAs in their sole discretion, ByteDance shall promptly allow the TTP to conduct security testing (e.g., static or dynamic testing or other generally accepted practices) of Source Code and Related Files and Executable Code via the DTC to ensure the security of the Source Code and Related Files and Executable Code.

9.15   Source Code and Related Files Alterations.

(1)   ByteDance shall retain the exclusive right to alter the Source Code and Related Files, subject to the requirements and prohibitions in this Agreement.

(2)   ByteDance shall promptly alter the Source Code and Related Files at the request of TTUSDS, the TTP, the Third-Party Monitor, or the CMAs, to ensure compliance with this Agreement, and shall submit a response and initial implementation plan to TTUSDS and the TTP within three (3) days of receipt of any such request, subject to the following:

(i)   If ByteDance rejects such a request, ByteDance shall submit the rejection and its rationale in writing to the TTP, the Security Committee, the Third-Party Monitor, and the CMAs promptly and, in any event, within one (1) day of the rejection;

(ii)   If ByteDance rejects such a request to alter the Source Code and Related Files, fails to alter the Source Code and Related Files as requested in a timely manner and consistent with the implementation plan, or fails to respond to the requested alteration within three (3) days, TTUSDS shall ensure the TTP, in coordination with the Third-Party Monitor, evaluates practicable options to ensure compliance with this Agreement absent the requested alteration. If after due consideration of all options, the TTP determines that there is no adequate option to ensure compliance with this Agreement without the requested Source Code and Related Files alteration, TTUSDS shall ensure the TTP, in consultation with the Security Committee, notifies ByteDance (the "**Suspension Notice**"), with a copy to the CMAs, the Third-Party Monitor, and the Security Committee, of the TTP's intent to suspend user access to the TikTok U.S. Platform, in whole or in part, in no less than two (2) days and no more than four (4) days (the period between the date of the notice and the suspension, the "**Remediation Window**"). TTUSDS shall ensure the TTP implements any suspension as set forth in a Suspension Notice upon expiration of the Remediation Window unless: (a) ByteDance has remediated the issue to the TTP's satisfaction in its sole discretion; (b) ByteDance has obtained a waiver from the CMAs; or (c) a majority of the Security Committee has determined and certified to the CMAs that the suspension is not necessary to ensure the Transaction Parties' compliance with this Agreement, accompanied by a reasoned and detailed analysis and explanation for the decision;

(iii)   At the request of the CMAs, TTUSDS shall ensure the TTP submits to the CMAs a confidential report regarding any rejected request pursuant to this Section 9.15, as well as any Security Committee override of a suspension; and

(iv)   If a suspension is implemented, once ByteDance provides Source Code and Related Files alterations to address the identified issue, TTUSDS shall ensure the TTP promptly reviews ByteDance's Source Code and Related Files alterations and, if acceptable to the TTP in its sole discretion, immediately reinstates user access to the TikTok U.S. Platform.

9.16   Location-Based Source Code Changes. Within thirty (30) days following the Operational Date, the Transaction Parties, in coordination with the TTP, shall, if necessary, update the Source Code and Related Files to reasonably ensure that TikTok U.S. Users physically located in the United States are restricted to the fullest extent possible from manipulating their geographic location within any version of the TikTok Global App to a country other than the United States, such that TikTok U.S. Users may solely use the TikTok U.S. App maintained and operated by the TTP. The Transaction Parties shall not take any action to degrade the user experience of TikTok U.S. Users in a manner designed to encourage TikTok U.S. Users to use a version of the TikTok Global App in a country other than the United States version, if multiple versions exist, or to log into the TikTok Global App not as a TikTok U.S. User.

9.17   Monitoring of TikTok U.S. App and TikTok U.S. Platform Interactions and Systems for Non-U.S. TikTok Users.

(1)   TTUSDS shall identify and monitor, and TTUSDS shall ensure the TTP identifies and monitors, for auditing purposes, all interactions and data elements exchanged between the TikTok U.S. App and TikTok U.S. Platform, on one hand, and systems operated by or on behalf of ByteDance serving non-U.S. TikTok Users, on the other hand. TTUSDS shall employ, and shall ensure that the TTP employs, technical means to block any such interactions that are unexpected or unauthorized, in the sole discretion of the TTP, and reports, within one (1) day of discovery and validation, any such interactions that have resulted or could reasonably result in unauthorized Access to, or other anomalous activity within, the TikTok U.S. App or the TikTok U.S. Platform to the Third-Party Monitor and the CMAs.

(2)   TTUSDS shall ensure the TTP identifies and monitors for auditing purposes all interactions and data elements exchanged between the TikTok U.S. App and TikTok U.S. Platform, on one hand, and any Internet host and any other system or infrastructure, on the other hand. TTUSDS shall ensure the TTP employs technical means to block any such interactions that are unexpected or unauthorized, in the sole discretion of the TTP, and reports, within one (1) day of discovery and validation, any such interactions that have resulted or could reasonably result in unauthorized Access to, or other anomalous activity within, the TikTok U.S. App or TikTok U.S. Platform to the Third-Party Monitor and CMAs.

(3)   The Transaction Parties shall ensure that encryption does not prevent the TTP from performing its obligations in connection with this Section 9.17.

(4)   To the extent that the TTP's identification and monitoring activities under Sections 9.17(1)–(2) conflict with General Data Protection Regulation ("**GDPR**") or other legal requirements, TTUSDS shall, within fourteen (14) days following the conflict arising: (i) provide written notice to the CMAs, including a detailed description of the legal requirements that create a conflict with citations to the relevant governing source(s); and (ii) coordinate with the TTP to present solutions to the CMAs that could be implemented to minimize the conflict to the greatest extent possible.

9.18   Ongoing Risk Analysis. TTUSDS shall ensure the TTP assesses on an ongoing basis the risks posed to the national security of the United States and the privacy of TikTok U.S. Users, based on analysis of Source Code and Related Files, architectural analysis, and analysis of data flows, and that the TTP reports such findings to the Security Committee, Third-Party Monitor, and CMAs on a quarterly basis.

9.19   TTP Communications. ByteDance shall not inhibit, and shall ensure that none of its Affiliates inhibit, whether through the MSA or other means, TTUSDS's or the TTP's ability to communicate with each other, with the Third-Party Monitor, with the CMAs, or with any other appropriate USG authority, in each case independently and without the involvement or awareness of ByteDance or its Affiliates.

ARTICLE X

TECHNOLOGY OFFICER

10.1   Technology Officers. The Transaction Parties shall ensure the TTP appoints one (1) or more technology officers (the "**Technology Officers**") in each country where TTP Personnel are performing responsibilities in connection with the MSA to serve as the primary liaisons between the TTP and the Third-Party Monitor and CMAs and that the MSA fully incorporates the requirements of this Article X.

10.2   Qualifications of the Technology Officers. The Transaction Parties shall ensure that each Technology Officer:

(1)   is a Resident Sole U.S. Citizen who has, or is eligible for, a U.S. personnel security clearance for any Technology Officer in the United States, and if not in the United States, is a citizen of their country of residence;

(2)   has the appropriate senior-level authority and resources within the TTP and the necessary technical skills and experience to ensure compliance with this Agreement and to fulfill all other obligations of the position;

(3)   has no current or prior employment, contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates;

(4)   has Physical Access and Logical Access to all of the facilities, systems, records, and meetings of the TTP; and

(5)   regularly has Physical Access to the DTC necessary to ensure compliance with this Agreement.

The Transaction Parties shall ensure that if any Technology Officer holds other titles and responsibilities beyond serving as a Technology Officer for the purposes of this Agreement, such other responsibilities do not prevent the Technology Officer from performing his or her

obligations in connection with this Agreement and that the Technology Officer remains an employee of the TTP.

10.3   Initial Nomination of the Technology Officer.

(1)   The appointment of each Technology Officer shall be subject to the prior non-objection of the CMAs. Within thirty (30) days following the Effective Date, the Transaction Parties shall ensure the TTP nominates each Technology Officer and submits complete Personal Identifier Information, a *curriculum vitae* or similar professional synopsis of the nominee, and any other information requested by the CMAs to assess whether the individual can effectively perform the obligations of the Technology Officer consistent with this Agreement. If the CMAs do not object within twenty-one (21) days following receipt of all necessary information about a nominee, the lack of action shall constitute a non-objection to that nominee. If the CMAs object, the Transaction Parties shall ensure the TTP nominates a different candidate within seven (7) days following receipt of any such objection, subject to the same procedures as the initial nomination. The Transaction Parties shall ensure the TTP appoints each Technology Officer within three (3) days following non-objection by the CMAs to that nominee.

10.4   Removal and Replacement.

(1)   The Transaction Parties shall ensure the TTP does not remove any Technology Officer without the prior non-objection of the CMAs. The Transaction Parties shall ensure the TTP notifies the CMAs at least fourteen (14) days before the proposed removal of a Technology Officer unless such removal is for cause, and such a removal shall only be proposed in conjunction with the nomination of a new candidate for the position, to prevent a vacancy from taking place, subject to the same procedures as the initial nomination. Such cause must consist of willful misconduct, gross negligence, reckless disregard, violation of applicable law, violation of company policy, or failure of the individual to perform his or her job duties. The Transaction Parties shall ensure the TTP does not remove any Technology Officer for the Technology Officer's actual or attempted efforts to comply with or ensure compliance with this Agreement.

(2)   Should the CMAs, in their sole discretion, determine that any Technology Officer has intentionally or through gross negligence failed to meet his or her obligations or has otherwise undermined the effectiveness of this Agreement, the CMAs may direct the TTP to remove such Technology Officer and the Transaction Parties shall ensure the TTP promptly, and in any event within two (2) days of such direction, removes such Technology Officer.

(3)   In the event of any vacancy in any Technology Officer position, the Transaction Parties shall ensure the TTP notifies the CMAs within one (1) day and, within fourteen (14) days following such vacancy occurring, nominates a replacement Technology Officer, subject to the same process as the initial nomination.

10.5   Communication with the Third-Party Monitor and CMAs. The Transaction Parties shall ensure that each Technology Officer maintains reasonable availability for discussions with the Third-Party Monitor and CMAs on matters relating to compliance with this

Agreement and has the ability to communicate with the Third-Party Monitor and CMAs independently and without the involvement or awareness of any of the Transaction Parties.

10.6   Reporting of Violations. The Transaction Parties shall ensure that each Technology Officer reports any actual or potential violation of this Agreement to the Security Officer, the Third-Party Monitor, and the CMAs as soon as practicable, but in any event within one (1) day of learning of the actual or potential violation.

10.7   Costs. The Transaction Parties shall be responsible for all costs associated with each Technology Officer.

ARTICLE XI

PROTECTED DATA

11.1   Excepted Data.

(1)   Any proposed change to the categories of Excepted Data under Section 1.11, including Annexes A, B, and C, as applicable, shall be subject to the prior written consent of the CMAs. Prior to making any such change, the Transaction Parties shall submit a request to the CMAs identifying the additional data fields and formats proposed to become Excepted Data and shall include in the request the rationale for their designation as Excepted Data and any other information requested by the CMAs, in their sole discretion, to assess the request. The Transaction Parties shall not treat, and shall ensure the TTP does not treat, any Protected Data as Excepted Data without the prior written consent of the CMAs. If a change involves the categories outlined in Section 1.11(2) or (3), the Transaction Parties shall update Annexes A, B, and C, as applicable, and submit such updated Annexes to the Third-Party Monitor and CMAs within three (3) days following the Transaction Parties' receipt of the CMAs' consent.

(2)   TTUSDS shall ensure that Excepted Data does not contain any Protected Data except in accordance with, as applicable, the fields and formats specified in Annexes A, B, and C before transmitting any Excepted Data to ByteDance, TikTok Inc., or their respective Affiliates, and shall make available, upon the request of the Third-Party Monitor or CMAs, evidence of compliance with this requirement. TTUSDS shall ensure that such evidence includes a review of logs from the gateways through which Excepted Data will transit, a review of system architecture to ensure those gateways are the sole transmission method for Excepted Data, and interviews with relevant TTUSDS and TTP Personnel. The Transaction Parties shall ensure that the Third-Party Monitor promptly, and in any event within one (1) day of discovery, reports to the CMAs any disclosure of Protected Data.

11.2   Public Data.

(1)   The Transaction Parties shall not add new Public Data feature categories or implement any such changes in the TikTok U.S. App to collect additional Public Data feature categories, unless and until all of the following conditions are met:

(i)   The Security Committee reviews and approves the designation of such feature categories as Public Data following a determination that public release of such feature categories is consistent with the privacy policy for the TikTok U.S. App (either existing or updated to address the release of such feature categories), the DPCP, and standard industry practice by U.S. social media companies, such as YouTube, Facebook, Instagram, and Twitter;

(ii)   The Transaction Parties provide notice to the Third-Party Monitor and CMAs, including an updated version of Annex E, highlighting any new feature categories designated as Public Data with a rationale for each addition and screenshots of the TikTok U.S. App from the perspective of a TikTok U.S. User demonstrating that the data will be generally public unless an individual user makes such data private, in which case such data shall remain Protected Data for such individual;

(iii)   TTUSDS provides notice using plain language to TikTok U.S. Users of any change to the privacy policy, if required, for the TikTok U.S. App, highlighting any new feature categories, and the rationale for making such change; and

(iv)   The Transaction Parties have resolved any objections raised by the CMAs with the additional feature categories. If the CMAs do not raise any objections within sixty (60) days following receipt of notice under Section 11.2(1)(ii), the lack of action shall constitute a non-objection.

(2)   The CMAs may raise objections to the collection of Public Data within approved feature categories or data fields within the feature categories by providing notice to the Security Committee. The Transaction Parties may explain why any such Public Data should remain public and the potential business and operational impact of changing it to Protected Data. If, after this process, the CMAs, in consultation with the Security Committee, determine that the relevant feature category or data field within a feature category should be re-designated as Protected Data, the Transaction Parties shall implement a plan to re-designate the applicable Public Data as Protected Data within ninety (90) days of receiving the request from the CMAs; *provided, however*, that such a re-designation shall not be required if the Security Committee confirms that such feature category or data field within a feature category is consistent, at the time of consideration, with the DPCP and standard industry practice by similar U.S. companies such as YouTube, Facebook, Instagram, and Twitter.

(3)   TTUSDS shall not provide, and shall ensure the TTP does not provide, to ByteDance or any of its Affiliates any reports or datasets providing insights into Public Data to a greater extent than what a public Internet user could reasonably view or ascertain, without the prior review and approval by the Security Committee. For the avoidance of doubt, the limitations in this Section 11.2(3) shall not restrict ByteDance or any of its Affiliates from receiving: (i) videos at a higher resolution than is ultimately published on the TikTok U.S. App;

47

(ii) other Public Data and/or datasets related to Public Data where the Public Data elements are accessible to Internet users, but not ordinarily in volumes and at speeds needed to operate the TikTok global platform; and (iii) any reports that otherwise can be or are produced by third parties based on or derived from Public Data.

11.3   Expatriate TikTok U.S. User Requests.

(1)   TTUSDS shall classify as a TikTok U.S. User any U.S. citizen who, upon registering through any version of the TikTok Global App, is not classified as a TikTok U.S. User and requests re-classification as a TikTok U.S. User, in accordance with a protocol to be developed by TTUSDS and subject to the prior non-objection of the CMAs (the "**Expatriate Request Protocol**"). At a minimum, TTUSDS shall ensure that such protocol provides for: (i) the option during new user registration on all versions of the TikTok Global App to allow U.S. citizens to select an option, and cause such user, to be re-classified as a TikTok U.S. User; (ii) sending a push notification to existing users of all versions of the TikTok Global App when first opened from a U.S. IP address notifying them of the option to be re-classified as a TikTok U.S. User if they are U.S. citizens; (iii) posting an article in the TikTok Global App Help Center regarding the option for U.S. citizens to be re-classified as a TikTok U.S. User; and (iv) including a feature within all versions of the TikTok Global App that enables users to select an option to be re-classified as a TikTok U.S. User if they are U.S. citizens. In order to minimize risks of conflicts of laws, TTUSDS may, subject to non-objection by the CMAs, implement a protocol that allows users outside the United States to present identification to a third party, who is not an Affiliate of ByteDance, that will confirm whether the user should be treated as a TikTok U.S. User. The Transaction Parties shall ensure that re-classification as a TikTok U.S. User is straightforward for users to find and complete.

(2)   By no later than the Operational Date, the Transaction Parties shall submit the Expatriate Request Protocol to the Third-Party Monitor and CMAs. If the CMAs do not object in writing within fourteen (14) days following receipt of the Expatriate Request Protocol, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Expatriate Request Protocol, the Transaction Parties shall address all concerns raised by the CMAs to the CMAs' satisfaction in a revised Expatriate Request Protocol submitted to the CMAs within fourteen (14) days following receipt of the written objection, which revisions shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial Expatriate Request Protocol. The Transaction Parties shall implement, and shall ensure the TTP implements, the Expatriate Request Protocol within three (3) days following the non-objection of the CMAs.

(3)   To the extent that a request or class of requests by U.S. Citizens to re-classify as TikTok U.S. Users pursuant to Section 11.3(1) conflicts with GDPR or other legal requirements, TTUSDS shall: (i) provide written notice to the Security Committee and Third-Party Monitor, including a detailed description of the legal requirements that create a conflict with citations to the relevant governing source(s); and (ii) coordinate with the TTP to present solutions to the Security Committee and Third-Party Monitor that could be implemented to minimize the conflict to the greatest extent possible. TTUSDS shall ensure that the Security

Committee consults quarterly with the CMAs regarding any such conflicts and works in good faith to address any concerns raised by the CMAs.

(4)   TTUSDS shall ensure that the Security Committee reviews all requests by users of the TikTok U.S. App or other versions of the TikTok Global App to de-classify as TikTok U.S. Users, and only approves such requests, with the balance weighed in favor of denial, where: (i) the user has not within the past sixty (60) days accessed the TikTok U.S. App or any other versions of the TikTok Global App from within the United States; and (ii) the user identifies his or her appropriate country of citizenship.

11.4   <u>End User Agreements and User Policies</u>. TikTok Inc. and TTUSDS shall submit advance notice to the CMAs of any intention to change materially the Terms of Service, with such materiality to be determined in consultation with the Third-Party Monitor, the privacy policy for the TikTok U.S. App, content moderation policy, or other published policies similar thereto (each, a "**User Agreement**") so the CMAs may review such User Agreements for consistency with this Agreement. Any material change, as determined in consultation with the Third-Party Monitor, to a User Agreement shall be subject to the prior non-objection of the CMAs except as otherwise provided herein. If the CMAs do not raise any objections within fifteen (15) days following receipt of the proposed change, the lack of action shall constitute a non-objection. TikTok Inc. and TTUSDS shall address all feedback from the CMAs prior to finalizing changes to any User Agreement; *provided, however*, that there shall be no limitation on finalizing such changes prior to the non-objection of the CMAs as long as TikTok Inc. and TTUSDS, as the case may be: (1) include in the original notice to the CMAs a clear explanation of the need for urgent implementation; and (2) address any feedback from the CMAs as promptly as possible after receipt. Notice to the CMAs pursuant to this Section 11.4 shall constitute notice only under this Section 11.4 and shall not satisfy any other notice requirements. Any feedback or non-objection by the CMAs under this Section 11.4 is specific to the change to the particular User Agreement and does not represent a USG determination applicable to any other context.

11.5   <u>Protected Data Storage</u>. The Transaction Parties shall ensure that all Protected Data, while such Protected Data remains in the possession of the Transaction Parties, is stored and remains: (1) exclusively in the United States, with no transmittal outside of the United States except as otherwise provided in this Agreement; and (2) within the TTP's secure cloud environment, both except as expressly provided in this Agreement or otherwise by the prior written consent of the CMAs. The Transaction Parties shall ensure that any Protected Data transferred to third parties (and therefore not in the possession of the Transaction Parties) is subject to the vendor reviews and policies under Article XIII. For the avoidance of doubt, Section 11.5(1) shall not prohibit TTUSDS Personnel in DTC Approved Countries from Accessing Protected Data through the TTP's secure cloud environment. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 11.5 to the Third-Party Monitor and CMAs.

11.6   <u>User Interaction Data Deletion</u>. The Transaction Parties shall ensure that all User Interaction Data in the possession of the Transaction Parties is deleted no later than eighteen (18) months after it is stored on the TikTok U.S. Platform or otherwise deleted in accordance with applicable law. For the avoidance of doubt, this deletion requirement applies to all data related

to individual users and their private interactions with content on the TikTok U.S. App (e.g.*,* data on specific individuals who viewed or liked a video) but does not apply to aggregated data (e.g.*,* the total number of views or likes a video has received).

11.7   Initial Transfer of Protected Data. By no later than the Operational Date, ByteDance shall transfer, and shall ensure that its Affiliates transfer, all Protected Data held by ByteDance and its Affiliates as of the Effective Date or acquired thereafter (collectively, the "**Legacy Protected Data**") to the TTP (the date of such transfer, the "**Transfer Date**"); *provided, however*, that if any Legacy Protected Data is subject to any litigation hold or legal preservation requirement as of the Transfer Date, ByteDance may transfer such Protected Data to a third-party approved in advance by the CMAs to hold such data in escrow pending satisfaction of the applicable litigation hold or legal preservation requirement. On or prior to the Transfer Date, ByteDance shall notify the CMAs in writing of any litigation hold or legal preservation requirement applicable to any Legacy Protected Data. ByteDance shall provide written confirmation to the Third-Party Monitor and CMAs promptly upon the successful transfer of all Legacy Protected Data, or report ByteDance's failure to transfer all Legacy Protected Data by the Transfer Date.

(1)   Within one-hundred twenty (120) days following confirmation that all Legacy Protected Data has been successfully transferred (the "**Deletion Date**"), ByteDance shall irretrievably destroy, or cause to be irretrievably destroyed, all Protected Data, including copies thereof, wherever located, in the possession or control of ByteDance or any of its Affiliates, in accordance with the "Clear" level articulated in the NIST principles for sanitization and destruction of data. ByteDance shall submit monthly reports to the Third-Party Monitor and CMAs on its progress destroying Protected Data by the deadline herein.

(2)   Within sixty (60) days following the Deletion Date, the Transaction Parties shall ensure that all assets and operations in the United States of the Transaction Parties and their respective Affiliates that support, or have supported, the TikTok U.S. App and TikTok U.S. Platform undergo one or more audits (each, a "**U.S. Deletion Audit**") to confirm the irretrievable destruction of all Protected Data. The auditor, timing, scope, and methodology of the U.S. Deletion Audits shall be subject to the prior non-objection of the CMAs. By no later than the Deletion Date, the Transaction Parties shall submit sufficient information regarding the proposed auditor and scope of the U.S. Deletion Audits for the CMAs to assess the nominee and proposal. If the CMAs do not object in writing to the nominee and proposal within twenty-one (21) days following receipt, the lack of action shall constitute a non-objection. The Transaction Parties shall ensure that the auditor starts the initial U.S. Deletion Audit within five (5) days following the CMAs' non-objection and completes the initial U.S. Deletion Audit consistent with the proposal. If the CMAs object to the proposed auditor or proposal, the Transaction Parties shall submit an alternative auditor or modified proposal, as applicable, which resolves the concerns raised to the CMAs' satisfaction, within fourteen (14) days following the Transaction Party's receipt of any such objection, subject to the same procedures as the initial review. The Transaction Parties shall ensure that the auditor provides the results of each U.S. Deletion Audit to the CMAs within three (3) days following its completion. The Transaction Parties shall take, and shall ensure that their respective Affiliates take, all remedial actions deemed necessary by

the auditor or CMAs, in their sole discretion, based upon the results of any U.S. Deletion Audit within thirty (30) days of its completion unless otherwise extended in writing by the CMAs (including shutting down IT systems that continue to store or provide Access to Protected Data until such time that all Protected Data is irretrievably destroyed). The Transaction Parties shall provide, and shall ensure that their respective Affiliates provide, the auditor with all Physical Access and Logical Access necessary to interview Personnel and to conduct the U.S. Deletion Audits within the scope approved by the CMAs, including Physical Access and Logical Access to inspect any IT systems, networks, hardware and software, data, communications systems, properties, records and documents, and correspondence in the possession or control of the Transaction Parties. The Transaction Parties shall be responsible for all costs and expenses in connection with the U.S. Deletion Audits.

(3)   Within sixty (60) days following the Deletion Date, ByteDance shall further certify, through verification processes developed in coordination with a third party retained by and at the sole expense of ByteDance and subject to the CMAs' approval, that all Protected Data has been irretrievably destroyed globally (the "**Global Deletion Verification**"). ByteDance shall take, and shall ensure that its Affiliates take, all remedial actions identified by the third party, in its sole discretion, as a result of the Global Deletion Verification within thirty (30) days of its completion unless otherwise extended in writing by the CMAs (including shutting down IT systems that continue to store or provide Access to Protected Data until such time that all Protected Data is irretrievably destroyed). ByteDance shall provide, and shall ensure that its Affiliates provide, the third party with all Physical Access and Logical Access necessary to conduct the Global Deletion Verification, including Physical Access and Logical Access to interview Personnel and to inspect any IT systems, networks, hardware and software, data, communications systems, properties, records and documents, and correspondence in the possession or control of the Transaction Parties. ByteDance shall deliver the certification of the Global Deletion Verification to the CMAs no later than fourteen (14) days following completion of the Global Deletion Verification. Thereafter, ByteDance shall annually certify, on behalf of itself and its Affiliates, to the CMAs that it does not possess, and cannot Access, any Protected Data or copies thereof.

11.8   Restricted Access to Protected Data. Following the Deletion Date, ByteDance and TikTok Inc. shall not take possession of or Access, and shall ensure that none of their respective Affiliates take possession of or Access, any Protected Data, whether Legacy Protected Data or Protected Data collected, derived, or stored on or after the Transfer Date, without the prior written consent of the CMAs. For the avoidance of doubt, this Section 11.8 shall not limit ByteDance's Access to Excepted Data or Public Data in accordance with this Agreement. TTUSDS shall ensure that Access to Protected Data is limited to those Personnel who require Access to fulfill their assigned job responsibilities. The Transaction Parties shall ensure the TTP implements controls and safeguards to ensure compliance with these requirements, including: (1) Physical and Logical Access controls necessary to safeguard Protected Data generally; and (2) the ability to refuse Logical Access by the Transaction Parties or any Affiliate thereof to Protected Data. In the event that a TTP is removed or replaced, TTUSDS shall ensure the previous TTP retains control of all Protected Data unless and until the CMAs consent to a new TTP or an alternate custodian of Protected Data. The Transaction Parties shall ensure the TTP

promptly reports any non-compliance with this Section 11.8 to the Third-Party Monitor and CMAs.

11.9   Limited Access to Protected Data. Notwithstanding the restrictions in Sections 11.8 and 11.10, in addition to TTUSDS Personnel who require Access to Protected Data to fulfill their assigned job responsibilities, certain Personnel of the Transaction Parties and their Affiliates may Access certain fields of Protected Data for the limited purposes of addressing legal and compliance matters and certain other emergency situations involving the health, safety, and security of TikTok users and the public in and outside the United States; *provided* that any such Access is strictly in accordance with a protocol (the "**Limited Access Protocol**") developed by the Transaction Parties and the TTP and subject to the prior non-objection of the CMAs.

(1)   In the Limited Access Protocol, the Transaction Parties shall, among other issues, identify all circumstances under which certain ByteDance or TikTok Inc. Personnel may Access Protected Data; the requirements related to those Personnel, including any citizenship, residency, location, and screening requirements; the particular fields and formats of the Protected Data such Personnel may Access; and the method for providing such Access to Protected Data, which shall be through a secure, auditable environment created and maintained by the TTP.

(2)   Prior to ByteDance, TikTok Inc., or any of their respective Affiliates having any Access to Protected Data under this Section 11.9, the Transaction Parties shall submit the Limited Access Protocols to the Third-Party Monitor and CMAs. If the CMAs do not object in writing within thirty (30) days following receipt of the Limited Access Protocol, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Limited Access Protocol, the Transaction Parties shall address all concerns raised by the CMAs to the CMAs' satisfaction in a revised Limited Access Protocol submitted to the CMAs within thirty (30) days following receipt of the written objection, which shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial Limited Access Protocol. The Transaction Parties shall fully implement, and shall ensure the TTP fully implements, the Limited Access Protocol prior to ByteDance, TikTok Inc., or any of their respective Affiliates having any Access to Protected Data under this Section 11.9. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with the Limited Access Protocol or this Section 11.9 to the Third-Party Monitor and CMAs.

11.10   Restricted Persons. The Transaction Parties shall not transfer, and shall ensure that none of their respective Affiliates or the TTP transfer, any Protected Data to any CFIUS Restricted Persons unless otherwise approved by the CMAs. The Transaction Parties shall ensure that any Protected Data transferred to third parties (and therefore not in the possession of the Transaction Parties) is subject to the vendor reviews and policies under Article XIII. The Transaction Parties shall ensure the TTP promptly reports any non-compliance with this Section 11.10 to the Third-Party Monitor and CMAs.

11.11   Separate Credentials. By no later than the Operational Date, TTUSDS shall ensure the TTP implements controls such that any Logical Access to Protected Data requires additional, separate credentials. TTUSDS shall ensure that the controls implemented jointly by the TTP via the MSA and TTUSDS require credentials that are based on security best practices

(e.g., multiple factors of authentication) and restrict Logical Access based on a Person's physical location to the fullest extent possible and need to Access Protected Data to fulfill his or her assigned job responsibilities, in order to ensure compliance with this Agreement. TTUSDS shall ensure the TTP only allows Personnel of the TTP and TTUSDS who need Access to fulfill their assigned job responsibilities, or other Persons only in accordance with the Limited Access Protocol or with prior written consent of the CMAs, to hold credentials that allow Logical Access to Protected Data.

11.12 <u>Data Security Certifications</u>. Each of the Transaction Parties shall submit, and shall ensure the TTP submits, to the CMAs, on a semiannual basis, a certification regarding its full compliance with this Agreement's requirements related to Protected Data.

11.13 <u>Training by the TTP</u>. TTUSDS shall ensure the TTP regularly, and not less than annually, trains the TTP's relevant Personnel (including training new relevant Personnel as part of the initial onboarding process) on the MSA and this Agreement's requirements related to Protected Data.

<u>ARTICLE XII</u>

<u>DATA PRIVACY AND CYBERSECURITY PROGRAM</u>

12.1 <u>Program Establishment</u>. TTUSDS shall establish and maintain, and shall ensure the TTP establishes and maintains, a comprehensive data privacy and cybersecurity program (each, a "**DPCP**") that shall include policies and procedures to ensure compliance with this Agreement, including measures to safeguard Protected Data, Excepted Data, and Public Data (each as within the respective possession of TTUSDS and the TTP) and to enforce the Physical Access and Logical Access restrictions and Source Code and Related Files security measures. For the avoidance of doubt, the TTP DPCP shall only apply with respect to the TTP's roles and responsibilities as defined by the MSA.

(1) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall develop the DPCP in accordance with standards developed or published by the following standards organizations and/or as further specified: (i) NIST, including NIST Special Publication 800-82, Guide to Industrial Control Systems (2015); (ii) the NIST Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1 (January 10, 2017); (iii) NIST Special Publications 800-53 and 800-171, Revision 4; (iv) ISO, including ISO/IEC 27001 and 27002 standards; (v) the successor versions of each of Section 12.1(1)(i)-(iv); (v) the Center for Internet Security; or (vi) another standards organization with provisions pertaining to data protection as communicated by the Third-Party Monitor or CMAs.

(2) TTUSDS, in coordination with the TTP and Third-Party Monitor, shall ensure that the DPCP includes, consistent with the framework on which it is based, provisions for: the encryption of all Protected Data, Excepted Data, and Public Data in transit and select Protected Data, Excepted Data, and Public Data at rest as identified in the DPCP; inventory of authorized devices, software, hardware, applications, and credentials; secure configurations of systems and devices; data recovery; security training; Physical Access and Logical Access

controls; log controls; incident detection, handling, and response; penetration testing; and other robust processes and protections necessary for the activities set forth in this Agreement, including the secure submission and inspection of Source Code and Related Files, persistent monitoring of interactions of the TikTok U.S. App and TikTok U.S. Platform, unauthorized Access to or transmission of Protected Data, and other requirements set forth under this Agreement.

        (3)   TTUSDS, in coordination with the Third-Party Monitor, shall ensure that the DPCP provides for independent IT systems, networks, communications systems, and other resources that are logically segregated from those of ByteDance or any of its Affiliates, and to which none of ByteDance or any of its Affiliates has any Access.

        (4)   TTUSDS, in coordination with the TTP and Third-Party Monitor, shall ensure that the DPCP provides for an annual vulnerability assessment of the TikTok U.S. App and TikTok U.S. Platform to be conducted by the TTP. TTUSDS shall ensure that the Security Officer and Technology Officer jointly report the findings of such vulnerability assessments to the Third-Party Monitor and CMAs, along with their plans to address any such findings.

        (5)   As part of the DPCP, TTUSDS shall develop, and shall ensure the TTP implements, a violation reporting plan requiring all Personnel to report actual or potential violations of this Agreement or the DPCP to the Security Officer (in the case of TTUSDS) or Technology Officer (in the case of the TTP). Such plan shall include protections against retaliation for all Personnel.

12.2   <u>Adoption</u>. The adoption of the DPCP shall be subject to the prior non-objection of the CMAs. TTUSDS, in coordination with the TTP and Third-Party Monitor, shall submit a draft of the DPCP to the CMAs within thirty (30) days following the Operational Date. If the CMAs do not object in writing to the draft DPCP within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the proposed DPCP, TTUSDS shall address, and shall ensure the TTP addresses, all concerns raised by the CMAs to the CMAs' satisfaction in a revised draft of the DPCP submitted to the CMAs within thirty (30) days following receipt of the written objection, which revised draft shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial draft. TTUSDS shall implement, and shall ensure the TTP implements, the DPCP within three (3) days following non-objection of the CMAs.

12.3   <u>Amendment</u>. If at any time TTUSDS (including the Security Committee), the TTP, or the CMAs determine that the DPCP should be amended, TTUSDS shall engage, in coordination with the TTP and Third-Party Monitor, with the CMAs to amend the DPCP. Any amendment of the DPCP shall be subject to the prior non-objection of the CMAs in accordance with the same procedures as the initial draft of the DPCP.

12.4   <u>Dissemination and Training</u>. Within thirty (30) days following the non-objection of the CMAs to the DPCP, TTUSDS shall disseminate, and shall ensure the TTP disseminates, the DPCP to all appropriate Personnel. TTUSDS, in coordination with the TTP, shall ensure that all appropriate existing and new Personnel of TTUSDS and the TTP receive training on the

DPCP (the "**Training**"). TTUSDS shall ensure that all appropriate new Personnel of TTUSDS and the TTP receive the DPCP and complete the Training, and that all such existing Personnel complete a refresher Training at least annually. TTUSDS shall ensure that the Security Officer (in the case of TTUSDS) and the Technology Officer (in the case of the TTP) implement and oversee the dissemination and Training processes.

12.5 Confidentiality. TTUSDS shall not share, and shall ensure the TTP does not share, the DPCP or any contents thereof with ByteDance or any of its Affiliates, including their respective Personnel, without the prior written consent of the CMAs.

12.6 Violations. TTUSDS shall ensure that the Security Officer and Technology Officer report any actual or potential violation of the DPCP and any remedial actions taken to the CMAs as soon as practicable, and in any event within one (1) day of discovery of the actual or potential violation. TTUSDS shall ensure that the Security Officer and Technology Officer each independently maintain a log of any reports received from individuals regarding perceived violations of the DPCP, whether or not ultimately reported to the CMAs. Any violation of the DPCP shall be deemed to constitute a violation of this Agreement, and the failure by TTUSDS or the TTP to obtain authorizations and approvals that are necessary to comply with the DPCP shall not excuse a violation of the DPCP.

ARTICLE XIII

VENDOR APPROVALS

13.1 Identification of Vendors. Within ninety (90) days following the Effective Date, the Transaction Parties shall submit to the Security Committee, Third-Party Monitor, and CMAs (or, if the Third-Party Monitor has not been engaged by the time of submission, within three (3) days following its engagement):

(1) a list and description of all third-party contracts and other arrangements as of the Effective Date with third parties that support or will support the TikTok U.S. App or the TikTok U.S. Platform, or that otherwise support TTUSDS and have Access to Protected Data or systems on which Protected Data is stored, or that otherwise provide for the sale of Protected Data, other than those on the Existing Vendors and Contracts List (as defined below).

(2) a list and description of contracts that are with the TTP or vendors directly contracted by the TTP as of the Effective Date (the lists and summaries identified in clauses (1) and (2) of this Section 13.1 collectively, the "**Existing Vendors and Contracts List**").

The Transaction Parties shall ensure that the Existing Vendors and Contracts List identifies the following information for each contract: the vendor (including its place of legal organization and principal place of business), the service provided, and any equipment supplied.

13.2 Thereafter, TTUSDS shall, periodically and no less frequently than semi-annually, review the same information described in Section 13.1(1) for each such contract, vendor, and other arrangement that is in place, update it as necessary to be accurate and complete

as of the date of review, and submit the updated information to the Third-Party Monitor (each such list, a "**Vendors and Contracts List**"). The Transaction Parties shall ensure that the Third-Party Monitor reviews the Existing Vendors and Contracts List used by TTUSDS and each Vendors and Contracts List and identifies all contracts that could permit a vendor to Access Protected Data or the TikTok U.S. Platform through TTUSDS (collectively, the "**Existing Vendor Contracts**") and notifies the Security Committee and the CMAs of all Existing Vendor Contracts. TTUSDS shall ensure that the Security Committee and Third-Party Monitor provide to the CMAs, within seven (7) days of a request by the CMAs, information regarding any current or prospective third-party vendors, contracts with third-party vendors, or information regarding the review of any current or prospective third-party vendor.

13.3   Review of Existing Vendor Contracts. TTUSDS shall ensure that, within forty-five (45) days following any submission under Section 13.1, the Security Committee evaluates all of the Existing Vendor Contracts, with review and oversight by the Third-Party Monitor, to determine if they are consistent with the obligations under this Agreement, and identify, in the Security Committee's sole discretion, any Existing Vendor Contracts that may allow for actions contrary to this Agreement and any information regarding any vendor party to any Existing Vendor Contract that causes the Security Committee to believe that the vendor's engagement under such Existing Vendor Contract has undermined, or would be reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, the vendor's ability to meet its obligations under such Existing Vendor Contract. In evaluating any Existing Vendor Contract, TTUSDS shall ensure that the Security Committee and Third-Party Monitor consider any concerns identified by the CMAs. TTUSDS shall ensure that, upon a conclusion by the Security Committee and Third-Party Monitor, or, in the event that the Security Committee and the Third-Party Monitor do not reach consensus, by the CMAs, that any Existing Vendor Contract undermines or is contrary to this Agreement or that information regarding any vendor party to an Existing Vendor Contract supports a concern that engagement of the vendor under an Existing Vendor Contract has undermined, or is reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, a concern that the vendor is unable to meet its obligations under an Existing Vendor Contract (each such determination, a "**Contrary Determination**"), the Security Committee and/or the Third-Party Monitor shall notify TTUSDS to which the Existing Vendor Contract relates, and TTUSDS shall immediately: (1) cause the termination or modification of such Existing Vendor Contract so that it no longer allows for actions contrary to this Agreement, as determined by the Security Committee and/or Third-Party Monitor in their sole discretion; (2) cause the termination of any role by a vendor party to such Existing Vendor Contract so that it is no longer a party to the Existing Vendor Contract; (3) take all actions necessary to end and prevent Logical Access to Protected Data or the TikTok U.S. Platform by the vendor at issue until a revised contract is executed or a new vendor is substituted, if applicable, that resolves the concerns of the Security Committee and Third-Party Monitor, in their sole discretion, and if applicable; and (4) notify the CMAs within three (3) days of the Contrary Determination.

(1)   Within fourteen (14) days following the later of the completion by the Security Committee and Third-Party Monitor of a review of Existing Vendor Contracts and by TTUSDS of action regarding any Contrary Determination, TTUSDS shall notify the Third-Party

Monitor and the CMAs of: (i) any Existing Vendor Contracts that have been terminated or modified; (ii) any vendors terminated as a party to an Existing Vendor Contract; (iii) the reason for such termination or modification; and (iv) all other actions taken to address a Contrary Determination.

13.4   New Vendor Contracts. TTUSDS shall not enter into, and shall ensure that its Affiliates do not enter into, any contract with a vendor that undermines or is contrary to this Agreement. TTUSDS, with the oversight of the Third-Party Monitor, shall ensure that the Security Committee continues to review all potential (other than routine commercial transactions between TTUSDS and advertising or e-commerce customers) contracts with new vendors or existing vendors providing a new type of service, in each case that will support the TikTok U.S. App, the TikTok U.S. Platform, or that otherwise support TTUSDS and have Access to Protected Data or systems on which Protected Data is stored (any such contract, a "**New Vendor Contract**"). TTUSDS shall ensure that the Security Committee notifies the Security Officer, Third-Party Monitor, and CMAs of any New Vendor Contracts that undermine or are contrary to this Agreement, including based on information regarding any vendor party to a New Vendor Contract that supports a concern that engagement of the vendor under a New Vendor Contract has undermined, or is reasonably likely to undermine, the effectiveness of this Agreement, including, as appropriate, a concern that the vendor will be unable to meet its obligations under a New Vendor Contract. Where the Security Committee determines that a potential New Vendor Contract is not consistent with this Agreement in its sole discretion, the Transaction Parties shall not execute such contract. Upon request by the CMAs, TTUSDS shall provide the CMAs with a list of New Vendor Contracts.

13.5   Vendor Program Policy. TTUSDS, in coordination with the Third-Party Monitor, shall implement a program (the "**Vendor Program**") whereby all New Vendor Contracts (including, for the avoidance of doubt, the vendors who are parties to such contracts) will be subject to initial and periodic review and non-objection by the Third-Party Monitor against criteria and risk factors to be identified, and TTUSDS shall adopt a written policy for the Vendor Program (the "**Vendor Program Policy**"), subject to the prior review and non-objection of the Security Committee and the CMAs. The Transaction Parties shall comply with the requirements of the Vendor Program Policy and shall share all necessary information with TTUSDS and the Third-Party Monitor to implement the Vendor Program Policy.

(1)   TTUSDS shall submit a draft Vendor Program Policy to the Third-Party Monitor and CMAs by no later than ninety (90) days following the Operational Date.

(2)   The adoption of the Vendor Program Policy shall be subject to the prior non-objection of the CMAs. If the CMAs do not object in writing to the draft Vendor Program Policy within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the draft Vendor Program Policy, TTUSDS shall address all concerns raised to the CMAs' satisfaction and submit a revised draft of the Vendor Program Policy to the CMAs within twenty-one (21) days following receipt of the written objection, which subsequent draft shall be subject to the same procedures as the initial draft. TTUSDS shall adopt the Vendor Program Policy within three (3) days following the non-objection of the CMAs. Upon adoption of the Vendor Program Policy, the Transaction Parties shall not execute,

finalize, or implement any New Vendor Contract that is inconsistent with the Vendor Program Policy, including the requirement to obtain the prior non-objection of the Third-Party Monitor. Any revisions or amendments to the Vendor Program Policy shall be subject to the prior non-objection of the CMAs, subject to the same procedures as the initial draft.

(3)   TTUSDS shall ensure that the Security Committee, with oversight by the Third-Party Monitor, oversees and maintains the Vendor Program Policy governing New Vendor Contracts to ensure compliance with this Agreement and the Vendor Program Policy. TTUSDS shall ensure that the Security Committee and the Third-Party Monitor have the authority to approve, reject, mitigate, or otherwise condition the engagement of any New Vendor Contract or any vendor party to a New Vendor Contract. TTUSDS shall ensure that any New Vendor Contract: (i) explicitly incorporates the requirements of this Agreement, as applicable, and (ii) provides TTUSDS with any contractual rights it will require to comply with the Vendor Program Policy, including to assess the risk factors set forth in the Vendor Program Policy and to periodically review third-party vendors.

(4)   TTUSDS shall ensure that the Security Committee and Third-Party Monitor considers any information provided by the CMAs regarding current or prospective New Vendor Contracts or vendors party to New Vendor Contracts and implements any recommendations from the CMAs regarding approving, rejecting, mitigating, or otherwise conditioning the engagement of any New Vendor Contract or any vendor party to a New Vendor Contract. To support any such recommendation, the CMAs may provide a justification to the Security Committee and Third-Party Monitor, based on relevant available unclassified information. To the extent that the recommendation is predicated on classified information, or other information that cannot be shared with the Security Committee and Third-Party Monitor, the CMAs may indicate so and share the relevant information with those Security Committee members, if any, who do possess the requisite qualifications for Access to such information.

(5)   TTUSDS shall ensure that the Vendor Policy Program, at a minimum, evaluates third-party vendors based on risk factors including: (a) the type, functionality and intended location of equipment, products, or services to be provided by the third-party vendor; (b) the intended usage and deployment of such equipment, products, or services to or within a DTC and the TikTok U.S. Platform; (c) the nature of Access to Protected Data, Source Code and Related Files, the TikTok U.S. Platform, or other sensitive operations of TTUSDS or the TTP to be granted to the third-party vendor; (d) the third-party vendor's record of compliance with relevant U.S. laws, regulations, standards, and contracts, as well as any applicable domestic or international data protection laws and regulations; (e) the third-party vendor's record of compliance with cybersecurity standards and any security breaches, to the extent known; (f) the country in which the third-party vendor maintains its principal place of business or conducts substantial operations; and (vi) any other risk factors identified by the Third-Party Monitor or CMAs in their sole discretion.

13.6   <u>CMA Waivers</u>. In connection with the review of the Existing Vendors and Contracts List, each Vendors and Contracts List, New Vendor Contracts, and the development and implementation of a Vendor Program Policy, TTUSDS may request, and the CMAs may

grant in their sole discretion, a waiver for any individual third-party vendors to be exempt for a specified period of time or completely from such future reviews.

13.7 TTP Access to Vendor Information. TTUSDS shall ensure the TTP has Access to all vendor information it needs to discharge its responsibilities under this Agreement. For the avoidance of doubt, there is a presumption that the sharing of commercially sensitive competitive pricing or related information shall not be necessary for the TTP to discharge its responsibilities under this Agreement.

ARTICLE XIV

CYBERSECURITY AUDITS

14.1 Cybersecurity Audit. TTUSDS shall engage, at its own expense, a U.S.-based independent third party that has no current or prior contractual, financial, or fiduciary relationship with ByteDance or any of its Affiliates, unless otherwise agreed to by the CMAs (the "**Cybersecurity Auditor**"), to conduct and complete a cybersecurity audit and prepare a report regarding its findings (the "**Cybersecurity Audit**"). TTUSDS shall, in coordination with the TTP, propose the terms, scope, methodology, and timeframe for completion of the Cybersecurity Audit (the "**Cybersecurity Audit Plan**"). The Cybersecurity Auditor and Cybersecurity Audit Plan shall be subject to the prior non-objection of the CMAs. TTUSDS shall ensure that the Cybersecurity Audit is undertaken in accordance with the Cybersecurity Audit Plan and includes an audit of each of the following:

  (1) the TTP's deployment of the TikTok U.S. Platform;

  (2) the establishment of the DTC and implementation of the DTC Operating Protocols;

  (3) TTUSDS's and the TTP's processes and tools for reviewing, inspecting, and compiling Source Code and Related Files and deployment of Executable Code in accordance with Section 9.10;

  (4) the identification of any vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files or Executable Code, and the remediation of such issues;

  (5) the implementation and effectiveness of the mobile sandbox for the TikTok U.S. App pursuant to Section 9.8;

  (6) the storage and protection of Protected Data, including verification of the newly created credentials for Logical Access to Protected Data and that none of the Transaction Parties has Access to Protected Data except as permitted under this Agreement;

APP-485

(7)   the secure and fully auditable environment through which Personnel of the ByteDance and its Affiliates may Access certain fields of Protected Data pursuant to the Limited Access Protocol; and

(8)   TTUSDS's and the TTP's implementation of and compliance with the DPCP.

14.2   Cybersecurity Auditor and Audit Plan.

(1)   Within one hundred and eighty (180) days following the Operational Date, TTUSDS shall submit to the CMAs the name of the proposed Cybersecurity Auditor, the proposed terms of engagement, and any other information requested by the CMAs to assess the proposal. If the CMAs do not object in writing within thirty (30) days following receipt of all necessary information, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to the proposed Cybersecurity Auditor or terms of engagement, TTUSDS shall, within fourteen (14) days following receipt of any such objection, propose a different Cybersecurity Auditor and make changes to the proposed terms of engagement, in each case subject to the same procedures as the initial proposal. If the CMAs object to the second proposed Cybersecurity Auditor, TTUSDS shall, within fourteen (14) days following receipt of such objection, propose three (3) Cybersecurity Auditors, from which the CMAs may select the Cybersecurity Auditor. TTUSDS shall engage the Cybersecurity Auditor within three (3) days following the non-objection of, or (if applicable) selection by, the CMAs.

(2)   TTUSDS, in coordination with the TTP and Third-Party Monitor, shall develop the Cybersecurity Audit Plan and, no later than twenty-one (21) days following the engagement of the Cybersecurity Auditor, submit the proposed Cybersecurity Audit Plan to the CMAs. If the CMAs do not object in writing within twenty-one (21) days following receipt of the Cybersecurity Audit Plan, the lack of action shall constitute a non-objection. If the CMAs object, TTUSDS shall, in coordination with the TTP and Third-Party Monitor and within fourteen (14) days following receipt of such objection, resolve all concerns raised by the CMAs and submit a revised Cybersecurity Audit Plan to the CMAs, subject to the same procedures as the initial proposal. TTUSDS shall ensure that the Cybersecurity Auditor fully completes the Cybersecurity Audit in accordance with the Cybersecurity Audit Plan.

14.3   Review of Findings. TTUSDS shall ensure that the Security Officer and Technology Officer, in consultation with the Security Committee, have the opportunity to review and comment on the preliminary findings of the Cybersecurity Audit. TTUSDS shall ensure that the Cybersecurity Auditor submits to the CMAs the preliminary and final Cybersecurity Audit report findings within three (3) days of the completion of each such report, and that the Security Officer and Technology Officer submit to the CMAs their responses to such reports.

14.4   Implementation Plan. Following completion of the Cybersecurity Audit and submission of the final Cybersecurity Audit report, TTUSDS shall ensure that the Security Officer submits to the CMAs a plan for implementing all recommendations arising from the Cybersecurity Audit within sixty (60) days following receipt of the final Cybersecurity Audit report. TTUSDS shall fully implement such plan within sixty (60) days following its submission

of its remediation plan to the CMAs, absent an objection by the CMAs to such plan or CMA approval for another timeline. If the CMAs object to the plan, TTUSDS shall resolve any concerns raised by the CMAs, including by submitting a revised implementation plan for CMA review if requested by the CMAs, within such reasonable period of time as determined by the CMAs in their sole discretion.

14.5   Additional Cybersecurity Audits. The CMAs may, in their sole discretion, require TTUSDS to undertake additional Cybersecurity Audits, subject to the same procedures as the initial Cybersecurity Audit, but no more than once (1) per year.

14.6   Costs of the Cybersecurity Audits. TTUSDS shall be responsible for all fees, costs, and expenses related to any Cybersecurity Audit.

ARTICLE XV

THIRD-PARTY AUDITS

15.1   Upon a request by the CMAs, but no more than once (1) per year, each Transaction Party shall, at its own expense, engage a U.S.-based third-party independent auditor (the "**Third-Party Auditor**") to assess its overall compliance with this Agreement (the "**Audit**"). For the avoidance of doubt, the Transaction Parties may propose the same third-party independent auditor. The relevant Transaction Party shall ensure that the Third-Party Auditor is available to meet and confer with the CMAs independent of any of the other Transaction Parties.

(1)   Review by CMAs. The Third-Party Auditor and the scope, methodology, and timeframe for completion of the Audit (the "**Audit Plan**") shall be subject to prior non-objection of the CMAs. The relevant Transaction Party shall submit sufficient information for the proposed Third-Party Auditor and Audit Plan for the CMAs to assess the nominee and proposal within thirty (30) days following the request of the CMAs. If the CMAs do not object in writing to the Third-Party Auditor and the Audit Plan within thirty (30) days following receipt, the lack of action shall constitute a non-objection. The relevant Transaction Party shall ensure that the Third-Party Auditor starts the Audit within five (5) days following the CMAs' non-objection and fully completes the Audit in accordance with the Audit Plan. If the CMAs object to the proposed Third-Party Auditor or Audit Plan, the Transaction Party shall submit an alternative Third-Party Auditor or modified Audit Plan, which in each case shall resolve the concerns raised to the CMAs' satisfaction, within fifteen (15) days following the Transaction Party's receipt of any such objection, subject to the same procedures as the initial nominee or proposal, as applicable. The Transaction Parties shall be responsible for all fees, costs, and expenses related to any Audits.

(2)   Audit Report. Each Transaction Party shall require the respective Third-Party Auditor to produce a written final Audit report, which shall include a list of any identified vulnerabilities or deficiencies that have affected or could affect such Transaction Party's compliance with this Agreement. The Transaction Party shall ensure that the audit report is provided to the Security Committee, the Security Officer, the Third-Party Monitor, and the

CMAs. The CMAs may require supplemental reports if any final audit report is not consistent with the CMAs' expectations related to the details of the analysis and conclusions presented.

ARTICLE XVI

THIRD-PARTY MONITOR

16.1   Engagement. Within thirty (30) days following the Effective Date, the Transaction Parties shall nominate an independent third-party monitor (the "**Third-Party Monitor**") to monitor the Transaction Parties' compliance with this Agreement and serve as a point of contact for the CMAs. The engagement of the Third-Party Monitor shall be subject to the prior non-objection of the CMAs. The Transaction Parties shall submit sufficient information to allow the CMAs to assess the nominee. If the CMAs do not object in writing within thirty (30) days following receipt of all information necessary to assess the nominee, as determined by the CMAs in their sole discretion, the lack of action shall constitute a non-objection. If the CMAs object to the proposed nominee, the Transaction Parties shall nominate a different candidate within five (5) days following receipt of any such objection, subject to the same procedures as the initial nomination. If the CMAs object to the second proposed Third-Party Monitor, within fourteen (14) days following receipt of such objection, the Transaction Parties shall propose three (3) candidates meeting the qualifications set forth in Section 16.2, from which the CMAs may select the Third-Party Monitor. TTUSDS shall engage the Third-Party Monitor within three (3) days following the non-objection of, or (if applicable) selection by, the CMAs. TTUSDS shall not remove or replace the Third-Party Monitor without the prior written consent of the CMAs, and TTUSDS shall nominate a replacement Third-Party Monitor within five (5) days following such removal, subject to the same procedures as the initial nomination. The CMAs, in their sole discretion, may direct TTUSDS to terminate the Third-Party Monitor and TTUSDS shall promptly, and in any event within three (3) days of such direction, terminate the Third-Party Monitor. In the event that there is a vacancy in the Third-Party Monitor position due to removal by the CMAs, resignation by the Third-Party Monitor, or otherwise, TTUSDS shall nominate a replacement Third-Party Monitor within twenty-one (21) days following such vacancy, subject to the same procedures as the initial nomination.

16.2   Qualifications. The Transaction Parties shall ensure that the Third-Party Monitor is an entity incorporated and with its principal place of business in the United States and uses only Resident U.S. Citizens to monitor compliance with this Agreement, in each case unless otherwise approved by the CMAs. The Transaction Parties shall ensure that the Third-Party Monitor possesses qualifications appropriate for monitoring compliance with this Agreement, including experience relevant to monitoring the obligations of this Agreement such as experience with: IT systems, cybersecurity, data privacy, social media platforms, content moderation, designing compliance programs, drafting policies and procedures for large companies, and related national security issues. For each Third-Party Monitor nominee, the Transaction Parties shall submit to the CMAs a detailed professional synopsis of the nominated Third-Party Monitor's experience, as well as any additional information requested by the CMAs. At the time of the nomination and for the duration of a Third-Party Monitor's engagement in connection with this Agreement, the Transaction Parties shall ensure that the nominated Third-Party Monitor has

no current or prior contractual, financial, or fiduciary relationship with any of the Transaction Parties or their Affiliates. TTUSDS shall ensure that the Third-Party Monitor, for the duration of its engagement in connection with this Agreement, does not owe any obligation to any of the Transaction Parties or their Affiliates that would limit the independence of the Third-Party Monitor or inhibit the Third-Party Monitor from sharing any information with the CMAs that the Third-Party Monitor or the CMAs deem relevant to ensuring the Transaction Parties' compliance with this Agreement.

16.3   Monitoring Agreement. TTUSDS shall negotiate a monitoring agreement (the "**Monitoring Agreement**") with each Third-Party Monitor. The execution of the Monitoring Agreement shall be subject to the prior non-objection of the CMAs. TTUSDS shall submit a draft of the Monitoring Agreement to the CMAs within ten (10) days following the non-objection of the CMAs to the Third-Party Monitor. If the CMAs do not object in writing to the draft Monitoring Agreement within thirty (30) days following receipt, the lack of action shall constitute a non-objection. If the CMAs object to the draft Monitoring Agreement, TTUSDS shall resolve the concerns to the satisfaction of the CMAs in the CMAs' sole discretion and submit a revised Monitoring Agreement to the CMAs within fourteen (14) days following receipt of the CMAs' comments, subject to the same procedures as the initial draft.

16.4   Within three (3) days following the non-objection of the CMAs to the Monitoring Agreement, TTUSDS shall enter into the Monitoring Agreement with the Third-Party Monitor. TTUSDS shall not amend or terminate the Monitoring Agreement without the prior written consent of the CMAs. TTUSDS shall ensure that the Monitoring Agreement includes at least the following terms:

(1)   the CMAs shall be third-party beneficiaries of the Monitoring Agreement;

(2)   the Third-Party Monitor shall report directly to the CMAs and shall owe a fiduciary duty to the CMAs;

(3)   the Third-Party Monitor shall owe no obligation to any of the Transaction Parties or any other Person that would limit the sharing of information with the CMAs that the Third-Party Monitor or the CMAs deem relevant, in the CMAs' sole discretion, to the Transaction Parties' compliance with this Agreement;

(4)   the Third-Party Monitor shall attend all meetings of the TTUSDS Board and the Security Committee, and otherwise review and observe TTUSDS's and the Security Committee's activities to ensure the security of Protected Data and that TTUSDS and the TTP do not engage in activities that undermine or are inconsistent with this Agreement;

(5)   the Third-Party Monitor shall monitor the relationships, communications, and interactions between ByteDance and its Affiliates, on the one hand, and TTUSDS, on the other hand, to ensure that any such relationships, communications, or interactions do not interfere with TTUSDS's independence and are consistent with this Agreement;

(6) the Third-Party Monitor may, in its sole discretion or at the direction of the CMAs, have the authority to conduct or trigger red or blue-team testing or exercises, the cost of which shall be borne by TTUSDS;

(7) the Third-Party Monitor shall inform the CMAs of any actual or potential violation of this Agreement within one (1) day of becoming aware of the actual or potential violation and shall provide, upon request, any information to the CMAs pertaining to the Transaction Parties' compliance with this Agreement;

(8) the Third-Party Monitor shall provide the CMAs with periodic reports as requested by the CMAs detailing the Transaction Parties' status implementing and complying with this Agreement, including any actual or potential violations of this Agreement;

(9) the Third-Party Monitor shall abide by the CMAs' guidance and protocols in performing its functions under this Agreement;

(10) the Third-Party Monitor shall have, and TTUSDS shall provide the Third-Party Monitor with, the complete ability to operate and have Access within TTUSDS in order to carry out its responsibilities under the Monitoring Agreement;

(11) the Third-Party Monitor shall not disclose any information it obtains in connection with the Monitoring Agreement or its services thereunder to any third party, except for the TTP, Source Code Inspector, Cybersecurity Auditor, or Third-Party Auditor as permitted under this Agreement, without the prior written consent of the CMAs;

(12) TTUSDS shall be responsible for all expenses and fees in connection with the Third-Party Monitor and the Monitoring Agreement;

(13) the Transaction Parties shall provide the Third-Party Monitor with any information that the Third-Party Monitor, in its sole discretion, deems necessary to verify compliance with this Agreement;

(14) upon the request of the CMAs, the Third-Party Monitor shall share with the CMAs any information provided to it from the Transaction Parties; and

(15) the CMAs, in their sole discretion, may direct TTUSDS to terminate the Third-Party Monitor at any time for any reason without approval from the Transaction Parties, and TTUSDS shall promptly, and in any event within three (3) days of such direction, terminate the Third-Party Monitor.

16.5 <u>Non-Retaliation</u>. None of the Transaction Parties shall take any retaliatory actions, including withholding payment, for actions taken by the Third-Party Monitor in order to evaluate and report on compliance with this Agreement.

16.6 <u>Responsibilities</u>. In addition to the responsibilities of the Third-Party Monitor set forth in this Agreement, TTUSDS shall ensure that the Third-Party Monitor takes all steps necessary to continuously monitor the Transaction Parties' compliance with this Agreement,

including through: regular interaction with the Transaction Parties' Personnel, including their management and directors, and the Security Officer, Compliance Officer, ByteDance POC, and Technology Officer; inspection of the Transaction Parties' documents, records, policies, and access logs; oversight of TTUSDS's operations involving IT systems, Protected Data, Source Code and Related Files, Content Moderation Processes, and vendors; and any other activities deemed necessary by the Third-Party Monitor to ensure the Transaction Parties' compliance with this Agreement.

16.7   Annual Performance Summary. TTUSDS shall ensure that the Third-Party Monitor submits to the CMAs, within seven (7) days following each anniversary of the Effective Date, a confidential annual performance summary (each, an "**Annual Performance Summary**"). None of the Transaction Parties shall, and the Transaction Parties shall ensure the TTP shall not, request or receive a copy of any Annual Performance Summary. Each Annual Performance Summary shall generally summarize the Third-Party Monitor's actions, decisions, and work performance, as well as the resources devoted to such efforts, from the prior year to carry out its obligations under the Monitoring Agreement, and also shall detail any restrictions experienced in carrying out its obligations. TTUSDS shall ensure that the Third-Party Monitor promptly addresses any questions from the CMAs regarding the Annual Performance Summary.

16.8   TikTok Inc. TikTok Inc. shall share documentation with the Third-Party Monitor, and grant the Third-Party Monitor Physical Access, which may be escorted, as requested by the Third-Party Monitor, in its sole discretion, to facilitate the Third-Party Monitor's assessment of the Transaction Parties' compliance with this Agreement.

ARTICLE XVII

CFIUS MONITORING AGENCY REVIEW AND INSPECTION RIGHTS

17.1   Access and Inspection. Upon one (1) day's notice, each of the Transaction Parties shall allow and afford the CMAs access to meet with its Personnel or the Personnel of its Affiliates, and to inspect the books and records, equipment, servers, and facilities, and premises owned, leased, managed, or operated in the United States by such Transaction Party or its Affiliates for the purposes of monitoring compliance with or enforcing this Agreement; *provided* that in exigent circumstances, no advance notice is required. This right to access and inspect extends to the Personnel, books and records, equipment, servers, facilities, and premises of any third-party contractor or agent working on behalf of any Transaction Party or its Affiliates. If any Transaction Party does not possess the authority or capability to afford such access, such Transaction Party shall use best efforts to obtain whatever is required from the third-party contractor or agent for such access to be afforded. Each of the Transaction Parties shall cooperate with the CMAs and promptly provide the CMAs with information as may be requested by the CMAs in their sole discretion to enforce and monitor compliance with this Agreement.

17.2   Access to the TTP. TTUSDS shall ensure, through the MSA, that the TTP provides Physical Access to and tours of its facilities to the CMAs, and facilitates meetings with its Personnel with the CMAs, for on-site reviews or audits during normal business hours to assess the implementation of this Agreement, and allows the CMAs to inspect company records

to verify compliance with this Agreement, in each case with no greater than one (1) day's prior notice. TTUSDS shall ensure, through the MSA, that the TTP cooperates with the CMAs and provides the CMAs with all information as may be requested by the CMAs, in their sole discretion, to enforce and monitor compliance with this Agreement.

ARTICLE XVIII

COMPLIANCE

18.1   Approvals and Authorizations. The Transaction Parties shall obtain and maintain, and shall ensure that their Affiliates obtain and maintain, all legal, statutory, regulatory, or other required authorizations and approvals, including those required by the government of the People's Republic of China, that are necessary to fully satisfy their obligations under this Agreement. Each of the Transaction Parties intends to be bound by all of the obligations under this Agreement regardless of impossibility or foreign compulsion and waives any and all defenses arising out of an inability to obtain any legal, statutory, regulatory, or other required authorization or approval necessary. The Transaction Parties shall promptly report to the Third-Party Monitor and CMAs any non-compliance with this Section 18.1.

18.2   Compliance Policies. Each of the Transaction Parties, in coordination with the Security Committee, the Security Officer, Compliance Officer, or ByteDance POC (as applicable to such Transaction Party), and the Third-Party Monitor, shall adopt and implement, and shall ensure that its respective Personnel follow, a separate compliance policy (each a "**Compliance Policy**") to govern its respective implementation of and compliance with this Agreement. Each Compliance Policy shall be subject to the prior non-objection of the CMAs. Each of the Transaction Parties shall submit a draft of its Compliance Policy to the CMAs within sixty (60) days following the Operational Date, resolve any concerns raised by the CMAs with respect to its Compliance Policy, and submit a revised draft to the CMAs within twenty-one (21) days following receipt of any comments from the CMAs. If the CMAs do not object within thirty (30) days following receipt of any draft of a Compliance Policy, the lack of action shall constitute a non-objection with respect to that Compliance Policy and the relevant Transaction Party shall formally adopt the Compliance Policy within three (3) days following the non-objection of the CMAs. TTUSDS shall ensure that the Security Officer and Security Committee are responsible for the oversight, implementation, and maintenance of the Compliance Policy for TTUSDS.

(1)   Each Transaction Party shall ensure that its respective Compliance Policy provides, at a minimum:

(i)   procedures for providing, receiving, and responding to information, reports, and requests from the TTP, Third-Party Monitor, and CMAs as required under this Agreement within the specified timelines;

(ii)   procedures for coordination between the relevant Transaction Party, its respective Affiliates, the TTP, the Security Committee, the Security Officer, the Content Advisory Council, the Technology Officer, the Source Code Inspector, the

66

Third-Party Monitor, the Cybersecurity Auditor, the Third-Party Auditor, and other designees and third parties as applicable and as required under this Agreement;

(iii)   procedures and requirements for facilitating all necessary Access by the TTP, Source Code Inspector, Third-Party Monitor, Cybersecurity Auditor, Third-Party Auditor, CMAs, and other third parties as applicable and as required under this Agreement;

(iv)   processes for informing and training its Personnel regarding this Agreement;

(v)   a notification and reporting policy to govern the prompt reporting of any actual or potential violation of this Agreement to the CMAs;

(vi)   guidance on the roles and responsibilities of relevant Personnel to ensure its compliance with this Agreement;

(vii)   a policy of non-retaliation for Personnel who report actual or potential violations of this Agreement;

(viii)   procedures for periodically reviewing and updating the Compliance Policy as needed to ensure compliance with this Agreement; and

(ix)   any other matters identified by the CMAs as necessary to ensure the Transaction Party's compliance with this Agreement.

(2)   TTUSDS shall ensure that its Compliance Policy includes procedures for the Security Officer to delegate his or her obligations under this Agreement in circumstances where the Security Officer is unavailable or requires assistance.

18.3   <u>CMA Approvals Required</u>. All protocols and policies required under this Agreement shall be subject to the prior non-objection of the CMAs, unless this Agreement expressly provides otherwise. The Transaction Parties shall not implement protocols and policies, or amend or modify such protocols and policies, without the prior non-objection of the CMAs. The Transaction Parties shall comply with the provisions of all protocols and policies that received the consent, non-objection, or approval of the CMAs under this Agreement. Any violation of the protocols and policies implemented pursuant to this Agreement shall be deemed to constitute a violation of this Agreement, and the failure by the Transaction Parties to obtain authorizations and approvals that are necessary to comply with such protocols and policies shall not excuse a violation thereof.

18.4   <u>Board Resolutions</u>. Each of the Transaction Parties shall ensure that its respective board of directors implements and maintains board resolutions as applicable and as necessary to enable and ensure compliance with this Agreement, and shall submit copies of such board resolutions to the Third-Party Monitor and CMAs within three (3) days following their adoption.

18.5   Quarterly Meetings. At the request of the CMAs, but not less than once every ninety (90) days unless waived in writing by the CMAs, the Transaction Parties shall meet, and shall ensure through the MSA that the TTP meets, with the Third-Party Monitor and CMAs at a mutually agreed upon time and location or by telephone (each such meeting, a "**Quarterly Meeting**"). At each Quarterly Meeting, the Transaction Parties shall provide, and shall ensure the TTP provides, all information requested, and answer all questions posed, by the Third-Party Monitor and CMAs. The CMAs may, in their sole discretion, exclude one or more of the Transaction Parties from all or part of a Quarterly Meeting. If the CMAs pose written questions to any Transaction Party or the TTP in advance of or following a Quarterly Meeting, such Transaction Party shall submit, and the Transaction Parties shall ensure the TTP submits, written responses to the CMAs within seven (7) days following receipt of the questions, unless otherwise extended by the CMAs.

18.6   Recordkeeping. The Transaction Parties shall ensure that the ByteDance POC, Compliance Officer, Security Officer, and Technology Officer create and maintain adequate records to monitor each of the Transaction Parties' and the TTP's respective compliance with this Agreement. If the TTP is replaced, the Transaction Parties shall ensure that the previous TTP retains copies of any records related to the performance of its obligations in connection with this Agreement and the MSA until advised otherwise by the CMAs.

18.7   Obligation to Report. The Transaction Parties shall: (1) require the ByteDance POC, Compliance Officer, Security Officer, and Technology Officer promptly, and in any event within one (1) day of discovery, to report any actual or potential violation of this Agreement to the Third-Party Monitor and CMAs; and (2) each maintain procedures that require Personnel to promptly inform the ByteDance POC, Compliance Officer, Security Officer, or Technology Officer, as applicable, of any actual or potential violation of this Agreement.

18.8   Defining a Violation. The CMAs may, in their sole discretion, provide interpretive guidance to the Transaction Parties and TTP as to what constitutes an actual or potential violation of this Agreement.

ARTICLE XIX

ANNUAL REPORTS

19.1   Annual Reports. Each of the Transaction Parties shall submit, within seven (7) days following each anniversary of the Effective Date, an annual report (each, an "**Annual Report**") to the Third-Party Monitor and CMAs that summarizes its compliance with this Agreement from the prior year, and includes, with respect to the preceding year:

(1)   organizational charts showing the equity and voting interests held in the entity, the dates of any transactions resulting in changes to such equity and voting interests, and with respect to ByteDance, a summary capitalization table identifying all shareholders holding more than one percent (1%) equity interest or voting interest in ByteDance as of the end of each quarter;

(2)   the address of the headquarters office location of the entity;

(3)   the full name (last, first, middle name) and telephone and email contact information for the ByteDance POC, the Compliance Officer, and the Security Officer, as applicable;

(4)   with respect to ByteDance, an organizational chart demonstrating and explaining which ByteDance Affiliates (including their location) perform work, services, operations, or support in relation to the TikTok U.S. App or TikTok U.S. Platform;

(5)   with respect to TTUSDS: (i) a summary of the funding provided by ByteDance; and (ii) a statement by TTUSDS regarding the sufficiency of such funds to perform its functions under this Agreement;

(6)   a certification of compliance with the hiring protocols required by Section 5.4;

(7)   a headcount of Personnel, and with respect to TTUSDS, a list of the names and titles of Key Management;

(8)   with respect to TTUSDS, the number of Personnel with a prior relationship with ByteDance or its Affiliates, and the percentage of such workforce within TTUSDS;

(9)   with respect to TTUSDS, a summary from the Security Committee of its activities from the prior year pursuant to this Agreement;

(10)   with respect to TTUSDS, a summary from the Content Advisory Council of its activities from the prior year pursuant to this Agreement;

(11)   current Architecture Diagrams, Data Flow Diagrams, and Source Code Review Diagrams;

(12)   a summary of any findings and reports of vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files, pursuant to Section 9.6;

(13)   a certification that all changes, updates, alterations, and improvements to the Source Code and Related Files were deployed to the TikTok U.S. App or TikTok U.S. Platform in accordance with the TTP's review and inspection processes pursuant to Section 9.10;

(14)   an update regarding any remediations or alterations to Source Code and Related Files made at the request of the TTP pursuant to Sections 9.10 or 9.15;

(15)   with respect to ByteDance, a certification that all individuals subject to classification as TikTok U.S. Users pursuant to Sections 1.35 and 11.3 are so classified as of the date of the Annual Report;

(16)   with respect to TTUSDS, a monthly breakdown of: (i) the total number of registered TikTok U.S. User accounts, and (ii) the number of TikTok U.S. Users who were monthly active users of the TikTok U.S. App;

(17)   a summary of any unexpected or unauthorized interactions pursuant to Section 9.17 and whether the circumstances permitting such interactions persist or have been resolved;

(18)   a summary of any changes or remediations made to the Recommendation Engine or Content Moderation Processes in response to issues identified by the TTP or Third-Party Monitor pursuant to Section 9.13;

(19)   a summary of all changes to Excepted Data and Public Data;

(20)   a certification that all Protected Data in the possession of the Transaction Parties is stored and subject to Access controls consistent with the requirements of this Article XI;

(21)   with respect to ByteDance, a certification, signed by a duly authorized representative, that none of ByteDance or its Affiliates holds, possesses, or has any Access to Protected Data in violation of this Agreement, or a summary of any findings of and remediations in relation to ByteDance or its Affiliates holding, possessing, or having any Access to Protected Data after the Deletion Date;

(22)   a summary of Access instances and compliance efforts in relation to the Limited Access Protocol, including the number of Personnel who used the Limited Access Protocol, their location, the reason for their Access, and the Protected Data Accessed;

(23)   with respect to TTUSDS, a summary of compliance efforts in relation to the DPCP, including Training;

(24)   with respect to TTUSDS, a summary of any actual or potential violations of the DPCP;

(25)   with respect to TTUSDS, updates regarding any remediation efforts in relation to findings from the Cybersecurity Audits conducted pursuant to Article XIV;

(26)   updates regarding any remediation efforts in relation to the Audits conducted pursuant to Article XV;

(27)   a summary of any challenges experienced in obtaining and maintaining the authorizations and approvals under Section 18.1, including any legal or regulatory changes affecting compliance with this Agreement;

(28)   a summary of any actual or potential violations of this Agreement and the remediation efforts in relation thereto;

(29)   as applicable, copies of the most recent versions of the DTC Operating Protocols, the Limited Access Protocol, the DPCP, Excepted Data, Public Data, and the Compliance Policies; and

(30)   any other subjects identified by the CMAs, in their sole discretion, as relevant to compliance with the Agreement.

19.2   TTUSDS shall ensure, through the MSA, that the TTP submits to the Third-Party Monitor and CMAs, within seven (7) days following each anniversary of the Effective Date, a confidential annual account (each, an "**Annual Account**") that summarizes the TTP's compliance with the requirements of this Agreement from the prior year, and includes, with respect to the preceding year:

(1)   current Architecture Diagrams, Data Flow Diagrams, and Source Code Review Diagrams;

(2)   a description of whether the TTP is sufficiently funded by the Transaction Parties;

(3)   a headcount of Personnel of the TTP whose job responsibilities are covered by the MSA and this Agreement;

(4)   a certification of compliance with the hiring protocols required by Section 5.4;

(5)   the number of Personnel with a prior relationship with ByteDance or its Affiliates, and the percentage of such workforce within the TTP;

(6)   a summary of any Physical Access to the DTC withheld by ByteDance or any of its Affiliates and the resolution of the same;

(7)   a statement as to the sufficiency of the DTC Operating Protocols in enabling the TTP to fully perform its obligations under the MSA and in connection with this Agreement;

(8)   a summary of any interference by ByteDance or any of its Affiliates with the TTP's Access to the DTC or Source Code and Related Files, or its inspection efforts in the DTC, and the resolution of the same;

(9)   a summary of any findings of vulnerabilities designated as high severity or equivalent, including any instance of Malicious Code in the Source Code and Related Files, pursuant to Section 9.6;

(10)   any changes to the TTP's processes, tools, and techniques used for reviewing and inspecting Source Code and Related Files and monitoring and blocking unexpected or unauthorized interactions pursuant to Article IX;

(11)   any deployment of Source Code and Related Files inconsistent with Section 10;

(12)   a summary of any findings that the Recommendation Engine operated inconsistently with the requirements under Section 9.13;

(13)   an update regarding any remediations or alterations to Source Code and Related Files made at the request of the TTP pursuant to Sections 9.10 or 9.15, and any issues with the Transaction Parties' obligation to address such requested remediations or alterations;

(14)   a summary of any unexpected or unauthorized interactions pursuant to Section 9.17 and whether the circumstances permitting such interactions persist or have been resolved;

(15)   the full name (last, first, middle name) and telephone and email contact information for the Technology Officer;

(16)   any indications that ByteDance or any of its Affiliates possessed or had Access to any Protected Data after the Deletion Date;

(17)   any issues with the restrictions on storage of and Access to Protected Data required under Article XI;

(18)   a summary of Training efforts pursuant to Sections 11.13 and 12.4;

(19)   a summary of any actual or potential violations of this Agreement and the remediation efforts in relation thereto; and

(20)   any other subjects identified by the CMAs, in their sole discretion, as relevant to compliance with the Agreement.

19.3   TTUSDS shall ensure the TTP does not provide any Annual Account to any of the Transaction Parties or their respective Affiliates.

19.4   Each of the Transaction Parties shall promptly submit, and shall ensure the TTP promptly submits, responses and relevant documentation to any requests by the CMAs for further or clarifying information regarding the content of any Annual Report or Annual Account.

ARTICLE XX

CONFIDENTIALITY

20.1   Confidentiality. This Agreement and all information provided by the Parties pursuant to this Agreement and the preceding term sheets will be accorded the confidential treatment required by Section 721(c) and 31 C.F.R. § 800.802 (2020).

20.2   <u>Public Summary</u>. Within seven (7) days following the Effective Date, ByteDance and its relevant Affiliates, including TikTok Inc., shall publish a press release and post on the Newsroom of their respective websites and their social media accounts a statement containing the summary of this Agreement at Annex G (the "**Public Summary**"). ByteDance hereby consents that the USG may also publicly disclose the Public Summary. The Transaction Parties shall consult in good faith on any amendments the CMAs may propose to the Public Summary, and the CMAs will consider in good faith any amendments the Transaction Parties may propose to the Public Summary.

20.3   <u>Accuracy Certification</u>. On the Effective Date, each of the Transaction Parties shall submit to the CMAs a certification that satisfies the requirements in Section 721(n) with respect to all information provided to CFIUS from May 27, 2020, through the Effective Date, including in connection with CFIUS Case 20-100 and this Agreement.

<u>ARTICLE XXI</u>

<u>REMEDIES</u>

21.1   <u>Penalties for Violations of the Agreement</u>. Each of the Transaction Parties acknowledges and agrees that if it violates any of the provisions of this Agreement, the Transaction Party may be liable to the United States for a civil penalty ("**Penalty**"), or subject to further action by the United States, consistent with 50 U.S.C. § 4565 and 31 C.F.R. §§ 800.901 and 800.902 (2020) for violations of mitigation agreements and conditions entered into or imposed under Section 721(*l*). The CMAs, in their sole discretion, may determine whether a violation has occurred, if such violation warrants the imposition of a Penalty or further action, and the appropriate Penalty amount or action, if any. The CMAs may consider a number of factors in determining the amount of a Penalty due for a violation of this Agreement, including the nature of the violation, the materiality of the violation, whether the conduct was willful or reckless, and the damage to the national security resulting from the violation.

21.2   <u>United States Government Remedies</u>. Each of the Transaction Parties acknowledges that if it fails to comply with any of the terms of this Agreement, the CMAs or any other appropriate USG authority may seek any and all remedies available under applicable law, including injunctive or other judicial relief, in addition to the remedies described in Section 21.1 of this Agreement. The taking of any action by the CMAs or other appropriate USG authority in the exercise of any remedy shall not be considered as a waiver by the CMAs or such other USG authority of any other rights or remedies. Nothing in this Agreement is intended to create rights to damages enforceable at law by the Transaction Parties against the USG, or to limit any rights the USG may have under law or regulation or this Agreement.

21.3   <u>Temporary Stop</u>. The Transaction Parties shall prevent, and shall ensure that their respective Affiliates and the TTP prevent, users from accessing the TikTok U.S. Platform (in each case, a "**Temporary Stop**") within three (3) days following the occurrence of any of the following:

(1)　　the failure by the Transaction Parties to establish TTUSDS and ensure that TTUSDS owns or has a license to, and manages, all of the assets and employs all of the Personnel related to the CFIUS Functions by the Operational Date in accordance with Article II;

(2)　　the failure by the Transaction Parties to ensure that TTUSDS becomes a Transaction Party to this Agreement by the Operational Date as required under Section 2.3;

(3)　　the failure by the Transaction Parties to execute a final MSA to which the CMAs have non-objected in accordance with the timelines under Section 8.2(1); *provided, however*, that a Temporary Stop shall not be required if: (i) the CMAs do not timely respond to an MSA submitted by the Transaction Parties due to a government shutdown; or (ii) the failure to execute the MSA is solely due to the TTP either having (a) failed to execute the MSA in a timely fashion, or (b) unreasonably withheld its consent;

(4)　　the failure by the Transaction Parties to execute a final MSA to which the CMAs have non-objected with a replacement TTP (i.e.*, not Oracle) in accordance with the timelines under Sections 8.2; *provided, however*, that a Temporary Stop shall not be required if: (i) the CMAs do not timely respond to an MSA submitted by the Transaction Parties due to a government shutdown; or (ii) the failure to execute the MSA is solely due to the replacement TTP either having (a) failed to execute or respond to the MSA draft in a timely fashion, or (b) unreasonably withheld its consent;

(5)　　notification to the CMAs by TTUSDS or the TTP that ByteDance and its Affiliates have not provided sufficient funds for TTUSDS or the TTP to perform their respective obligations in connection with this Agreement in accordance with Section 2.8 (with respect to TTUSDS) and Section 9.10(3) (with respect to the TTP); *provided* that*: (i) TTUSDS or the TTP has first notified ByteDance of the insufficiency and ByteDance has not resolved such insufficiency to the satisfaction of TTUSDS or the TTP, as applicable, within a timely manner; and (ii) after the CMAs have consulted with ByteDance regarding such notification of insufficiency, the CMAs do not provide their written determination that such circumstances do not warrant a Temporary Stop;

(6)　　notification to the CMAs by the TTP that it has been denied Physical Access to the DTC or Logical Access to review or inspect Source Code and Related Files, or that ByteDance has interfered with the TTP's inspection activities, in violation of the DTC Operating Protocols or Section 9.3, unless the CMAs provide their written determination that such circumstances do not warrant a Temporary Stop;

(7)　　notification to the CMAs by the TTP of the deployment to the TikTok U.S. App or TikTok U.S. Platform of any changes, updates, alterations, or improvements to the Source Code and Related Files that were not reviewed and inspected by the TTP in accordance with Section 9.10, including the requirement that only Source Code and Related Files for which the SBOM or its equivalent has been digitally signed by the TTP is deployed to the TikTok U.S. App or TikTok U.S. Platform;

(8)   notification to the CMAs by the TTP of the failure to, within 120 days of the Operational Date, incorporate into the Source Code and Related Files for the TikTok U.S. App a protective solution in accordance with Section 9.8;

(9)   notification to the CMAs by the TTP, or any results of the U.S. Deletion Audits, Global Deletion Verification, Cybersecurity Audits, Third-Party Audits, or any other audits or monitoring activities performed pursuant to this Agreement, that indicate that ByteDance or any of its Affiliates, intentionally or through gross negligence, did not irretrievably destroy Protected Data as of the Deletion Date or that ByteDance or any of its Affiliates, intentionally or through gross negligence, maintained or maintains Access to Protected Data after the Deletion Date;

(10)   notification to the CMAs by the TTP that Protected Data is not stored or subject to Access controls in accordance with Article XI, unless the CMAs provide their written determination that such circumstances do not warrant a Temporary Stop;

(11)   the failure by any of the Transaction Parties to remove any individual or entity appointed to any role under this Agreement at the written direction of the CMAs in accordance with the processes for such removals under this Agreement; or

(12)   the failure by the Transaction Parties or any of their Affiliates to obtain and maintain all legal, statutory, regulatory, or other required authorizations and approvals, including those required by the government of the People's Republic of China, in a manner that prevents the Transaction Parties or any of their Affiliates from fulfilling their obligations under this Agreement in violation of Section 18.1.

For the avoidance of doubt, as part of a Temporary Stop the Transaction Parties, their Affiliates, and the TTP may allow TikTok users who are not TikTok U.S. Users to access a TikTok platform other than the TikTok U.S. platform.

21.4   <u>Lifting a Temporary Stop</u>. Upon the occurrence of a Temporary Stop, the Transaction Parties shall not resume, and shall ensure the TTP does not resume, allowing users to access the TikTok U.S. Platform until the Transaction Parties have received the written consent of the CMAs to resume such access, upon the CMAs' finding, in their sole discretion, that the event triggering the Temporary Stop has been remedied or otherwise addressed to the satisfaction of the CMAs.

21.5   <u>Suspension of Service</u>. If the Transaction Parties or their Affiliates do not fully implement a Temporary Stop as required under Section 21.44, the CMAs may direct the TTP to suspend, and the Transaction Parties shall ensure through the MSA that the TTP suspends, user access to the TikTok U.S. Platform until the TTP has received the written consent of the CMAs to lift such suspension.

APP-501

ARTICLE XXII

GENERAL PROVISIONS

22.1   <u>Effectiveness</u>. Except as otherwise specifically provided in this Agreement, the obligations imposed by this Agreement shall take effect immediately upon the Effective Date and shall remain in effect until this Agreement is terminated in accordance with the terms hereof.

22.2   <u>Valid and Binding Obligation</u>. Each Transaction Party agrees that this Agreement constitutes a legal, valid, and binding obligation of such Transaction Party, enforceable against such Transaction Party in accordance with its terms. Each Transaction Party hereby irrevocably and unconditionally waives, to the fullest extent permitted by applicable law, any and all legal, equitable and other defenses to the enforcement of this Agreement or any obligation hereunder it may have (now or in the future) by reason of any illegality or lack of validity or enforceability of this Agreement or any obligation hereunder.

22.3   <u>Release</u>. Upon the execution this Agreement, each of the Transaction Parties, for itself, its administrators, heirs, representatives, successors, or assigns, hereby waives, releases, abandons, and forever discharges CFIUS and its successors, the United States, and any department, agency, or establishment of the United States, and any officers, employees, agents, successors, or assigns of such department, agency, or establishment, from any and all claims, demands and causes of action of every kind, nature, or description, whether known or unknown, which have been, could have been, or could be asserted in connection with CFIUS Case 20-100 or any related orders (including the August 14 Order), regardless of whether they were named in any complaints filed by the Transaction Parties and regardless of whether they were included in the complaint, including any claims for costs, expenses, attorney fees, and damages of any sort.

In connection with such waiver and relinquishment, each of the Transaction Parties acknowledges that it is aware that it may hereafter discover claims presently unknown or unsuspected, or facts in addition to or different from those which it now knows, with respect to the matters released herein. Nevertheless, it is the intention of each of the Transaction Parties, through such release, and with the advice of counsel, to settle and release all such matters, and all claims as described above relative thereto, which heretofore have existed, now exist, or hereafter may exist between the Transaction Parties and CFIUS, the United States, and any department, agency, or establishment of the United States, and officers, agents, employees and former employees, individually or in their official capacities, arising out of or related to any or all of this Agreement, CFIUS Case 20-100, or any related orders (including the August 14 Order); *provided, however*, that nothing herein shall operate to release or discharge any claim for breach of this Agreement.

22.4   <u>Interpretation</u>. The section headings and numbering in this Agreement are inserted for convenience only and shall not affect the meaning or interpretation of the terms of this Agreement. All references herein to Articles, Sections, and Annexes shall be deemed references to Articles, Sections, and Annexes of this Agreement unless the context shall otherwise require. The words "hereof," "herein," and "hereunder" and words of like import used in this Agreement refer to this Agreement as a whole and not to any particular provision of this

APP-502

Agreement. Whenever the words "include," "includes," or "including" are used in this Agreement they shall be deemed to be followed by the words "without limitation." The word "extent" in the phrase "to the extent" means the degree to which a subject or other thing extends and such phrase shall not mean simply "if." Whenever any provision in this Agreement refers to action to be taken by any Person, or which any Person is prohibited from taking, such provision shall be applicable whether such action is taken directly or indirectly by such Person. The definitions given for terms in this Agreement shall apply equally to both the singular and plural forms of the terms defined.

22.5   Notice Regarding Legal Representation. The Transaction Parties shall provide notice to the CMAs, including contact information, of any legal representation in connection with obligations under this Agreement, whether outside legal counsel or internal general counsel, within five (5) days following the Effective Date and thereafter within five (5) days following any change to such legal representation.

22.6   Choice of Law. This Agreement shall be governed by and interpreted according to the federal laws of the United States.

22.7   Direct Communications. The Transaction Parties acknowledge that the CMAs may communicate directly with the Security Committee, the ByteDance POC, the Compliance Officer, the Security Officer, the Technology Officer and TTP, the Source Code Inspector, the Third-Party Auditor, the Third-Party Monitor, the Cybersecurity Auditor, and any point of contact designated by the Transaction Parties. The Transaction Parties further acknowledge that the CMAs may communicate directly with any Personnel who initiate or are included on communications with the CMAs regarding this Agreement. These acknowledgments shall in no way prohibit or otherwise restrict the Transaction Parties from consulting with, obtaining advice from, or communicating with the CMAs through counsel.

22.8   Forum Selection. A civil action brought by any Party for judicial relief with respect to any dispute or matter whatsoever arising under, in connection with, or incident to, this Agreement shall be brought, if at all, in accordance with Section 721(e)(2) to the extent applicable. If Section 721(e)(2) is not applicable, such civil action shall be brought in the U.S. District Court for the District of Columbia.

22.9   Other Laws. Nothing in this Agreement is intended to limit, alter, or constitute a waiver of:

(1)   any obligation imposed on the Transaction Parties by any U.S. federal, State, or local law;

(2)   any enforcement authority available under any U.S. federal, State, or local law;

(3)   the sovereign immunity of the United States; or

(4)   any authority or jurisdiction the USG may possess over the activities of the Transaction Parties or their agents located within or outside the United States.

22.10   Conflict with Applicable Laws. In the event that any provision of law to which the Transaction Parties are subject is inconsistent with any provision of this Agreement, the Transaction Parties shall immediately notify the CMAs of the discrepancy and resolve the conflict to the satisfaction of the CMAs.

22.11   Change in Circumstances. If, after this Agreement takes effect, the CMAs or the Transaction Parties believe that changed circumstances warrant a modification or termination of this Agreement (including if the CMAs determine that the terms of this Agreement are inadequate or no longer necessary to address national security concerns), then the Transaction Parties shall negotiate in good faith with the CMAs to modify or terminate this Agreement. For the avoidance of doubt, if any of the Transaction Parties completes an initial public offering or if a sale or transfer of any Transaction Party to any Person that is not a foreign person (as defined at 31 C.F.R. § 800.224 (2020)) occurs, the Transaction Parties may petition the CMAs for a modification or termination (in the event of a requested termination, pursuant to Section 22.15) of this Agreement, which modification or termination shall be in the sole discretion of the CMAs. Rejection of a proposed modification alone does not constitute evidence of a failure to negotiate in good faith.

22.12   Severability. The provisions of this Agreement shall be severable, and if any provision hereof or the application of such provision under any circumstances is held invalid by a court of competent jurisdiction, it shall not affect the validity or enforceability of any other provision of this Agreement or the application of any other provision, which shall remain in full force and effect.

22.13   Waivers. The failure of the CMAs to insist on strict performance of any of the provisions of this Agreement, or to exercise any right granted herein, shall not be construed as a relinquishment or future waiver; rather, the provision or right shall continue in full force. No waiver by the CMAs of any provision of, or right under, this Agreement shall be valid unless it is in writing and expressly provides for the waiver of a specified requirement under a particular provision of this Agreement. The CMAs shall have the authority to grant or revoke any waiver, exception, consent, or approval in their sole discretion. The Transaction Parties understand and acknowledge that the CMAs will consider requests for a waiver or exception to any provision of this Agreement with a presumption of denial.

22.14   Successors and Assigns. This Agreement is binding upon, and inures to the benefit of, the Transaction Parties and their respective successors and assigns. For purposes of this Agreement, successors and assigns under this Section includes any corporate name changes. No Transaction Party may assign any obligation under this Agreement without the prior written consent of the CMAs. The Transaction Parties shall remain liable for all obligations under this Agreement that are assigned to any other Person. In the event that any Transaction Party effects the transfer, separation, or sale of a material portion of its business operations or assets that are subject to requirements under this Agreement, including by way of a sale of assets, spin-off, split-off, reorganization, or similar transaction, such Transaction Party shall immediately notify

the CMAs in writing and, after consultation with the CMAs, the transferee, successor, or acquirer, as applicable, may, without any further action required of the Transaction Parties, execute a joinder agreement under which such transferee, successor, or acquirer, as applicable, takes on the relevant obligations under this Agreement and becomes a Party hereto. In the event that any Transaction Party effects the transfer, separation, or sale of a material portion of its business operations or assets that are subject to requirements under this Agreement to an Affiliate, such Transaction Party shall, at the time of such transaction, cause the relevant Affiliate to execute a joinder agreement under which the Affiliate takes on the relevant obligations under this Agreement and becomes a Party hereto.

22.15   Termination of this Agreement. After this Agreement takes effect, it shall terminate only upon written notice by the CMAs to the Transaction Parties. Termination of this Agreement shall not relieve a Transaction Party from liability for any breach or violation of this Agreement occurring while the Agreement was in effect or for fraud. Article I (Definition of Terms) and Article XXII (General Provisions) shall survive a termination of this Agreement.

22.16   Amendment. This Agreement may be amended only by written agreement signed by all of the Parties.

22.17   Tolling of Deadlines. Any non-objection, consent, or approval provision applicable to the CMAs under this Agreement shall be tolled during a shutdown in federal government operations due to a lapse in appropriations.

22.18   Computing Time. All references to "days" in this Agreement mean calendar days unless otherwise expressly provided. In computing any time period pursuant to this Agreement:

(1)   For any period stated in days:

(i)   the day of the event that triggers the period is excluded; and

(ii)   the last day of the period is included, but if the last day is a Saturday, Sunday, or federal holiday, the period continues to run until the end of the next day that is not a Saturday, Sunday, or federal holiday.

(2)   For any period stated in "months," such period means once every thirty (30) days.

(3)   For any period stated in "quarters," such period means once every ninety (90) days.

(4)   For any period stated in "years," such period means once every three hundred and sixty-five (365) days.

(5)   For any period stated "semi-annually," such period means twice per year.

22.19   Notices. All notices and other communications given or made relating to this Agreement shall be in writing, shall be deemed to have been duly given or made as of the date of

receipt, and shall be sent by electronic mail addressed to the Parties' designated representatives at the addresses shown below, or to such other representatives at such other addresses as the applicable Party may designate in accordance with this Section:

If to the CMAs:

[XXX]

If to TTUSDS:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to TikTok Inc.:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to TikTok Ltd.:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

If to ByteDance:

[XXX]

With a copy to (which shall not constitute notice):

[XXX]

22.20   Entire Agreement. This Agreement, together with any Annexes and Exhibits hereto, constitutes the entire understandings of the Parties hereto and supersedes all prior agreements or understandings with respect to the subject matter hereof.

22.21   Counterparts. This Agreement may be executed in one (1) or more counterparts, including portable document format (.pdf) or other electronic counterparts, each of which shall be deemed an original, but all of which together shall be deemed to constitute one and the same agreement.

This Agreement is executed on behalf of the Parties:

ByteDance Ltd.

Date: _____   By: _____
                                     Printed Name:
                                     Title:

TikTok Ltd.

Date: _____   By: _____
                                     Printed Name:
                                     Title:

TikTok Inc.

Date: _____   By: _____
                                     Printed Name:
                                     Title:

TTUSDS

Date: _____   By: _____
                                     Printed Name:
                                     Title:

For [•]

Date: _____   By: _____
                                     Printed Name:
                                     Title:

For [•]

Date: _____   By: _____
                                  Printed Name:
                                  Title:

For [•]

Date: _____   By: _____
                                  Printed Name:
                                  Title:

APP-509

ANNEX A – Engineering and Business Related Metrics

ANNEX B – Interoperability Data

Annex C – E-Commerce Data

Annex D – Form of Joinder Agreement for TTUSDS

Annex E – Feature Categories as of the Effective Date

ANNEX F – List of ByteDance Competitors

ANNEX G – Public Summary

APP-516

Updated Definition of Terms Used in Annexes A and B

This table lists and defines various terms used in the descriptions laid out in Annexes A and B to the Term Sheet, related to Engineering and Business Related data and Interoperability data, respectively. Note that consistent with the categories laid out in Annex A, this data will be aggregated and will not contain identifiable information.

Term	Definition
3P data sharing requested	advertising engagement behavior (*e.g.*, views and clicks of an advertisement) that is shared with third-party partners to measure advertising performance
Account property	user account data (*e.g.*, register time, signature, number of videos published, number of followers)
Account status	indicates the status of the user account (*e.g.*, registered, unregistered, banned)
Action placement and history	data on each step of the user engagement funnel (*e.g.*, how many users start recording video, then edit their video, then publish their video); allows measurement of the total click-through rate and loss rate of each step
Action source user attributes	user behavior attributes (*e.g.*, 'live_duration_d30_avg_layer_byda_v1', which is calculated by the host's 30 day average live streaming duration time)
Activity attributes	data related to the attributes of live streaming activity (*e.g.*, activity name, activity time)
Addebug	data from each module in the advertising process that enables advertising optimization
Ads attributes	data related to the attributes of an advertising campaign (*e.g.*, advertising objective, targeting criteria, bidding settings, delivery schedule)
Ad property	data related to the creative aspects of an advertising campaign (*e.g.*, content, graphics, text, comments)
Ads experiment attributes	data related to the attributes of an advertising campaign experiment (*e.g.*, advertising objective, targeting criteria, bidding settings, delivery schedule, experiment details)
Ads review attributes	indicates whether a specific advertisement has passed or failed the advertisement review process and the associated reason (*e.g.,* "rejected because of violence content")
Ads tracking option	indicates an option for sending engagement behavior data between users and advertisements to third-party partners (*e.g..* domain name)
Adset property	Same as "Ad property"

APP-517

Agency property	segmented user acquisition metrics (*e.g.*, installs, retention, cost) by advertising agency names
Anchor fans range	a range indicating the number of fans identified in a live-streaming anchor (an anchor is a special link on a video that enables users to enter an application or website if the user is interested in a deeper exploration of related content within a video. It's composed of 3 basic parts: icon, title, landing page)
App attributes	app installation package attributes (*e.g.*, app version, app name)
App page	indicates which of the two potential app homescreens is designated (*i.e.,* the "For You" page or the "Following" page)
App property	basic information of the application (*e.g.*, app id, app version, iOS/Android)
Arbit trigger	indicates whether a push is triggered by Arbit (Arbit is the name of a system that triggers content/video pushes by the push algorithm)
Basic user interaction	commonly used aggregated metrics of user engagement with advertisements (*e.g.*, impression, click, video play)
Bid	offer by an advertiser of a specific price for a unit of result for their advertisement groups (*e.g.,* a system generated id which equates to "paying $15 for 1K impressions")
Bidding (settings)	settings that allow advertisers to set their bid strategy (for further information on bid strategies, see https://ads.tiktok.com/help/article?aid=9685)
Campaign property	segmented paid advertisement metrics by campaign names
Channel	type of subdivision for media source traffic (*e.g.*, Google can be divided into search channel and YouTube channel)
Channel property	same as "Channel"
Client interaction	actions taken by a user through the TikTok app or website (*e.g.*, like, save, favorite, watch video to completion)
Comment push off/on	indicates whether a user has turned on push notification for comments
Content type	type of content (*e.g.,* video, music, user card, comment, live streaming)
Conversion (settings)	settings that allow advertisers to set a conversion goal for their advertisement groups from the conversion types
Conversion type	type of conversion goal advertisers set for their advertisement groups (*e.g.,* app download, installation, activation, registration)
Coarse location	information that describes the location of a device with lower resolution than a latitude and longitude with three or more decimal places

2

APP-518

Comment attributes	action types such as comment posts and comment likes; comment characteristics (*e.g.*, whether the comment is spam, whether the comment is posted by friends)
Creative	reference to the specific images or videos that are presented to users, to facilitate evaluation of how users responded to that specific image or video advertisement
Creative property	creative characteristics (*e.g.*, creative media types, including image, video and text)
Creator power of influence	measurement of creator's influence (*e.g.*, how many followers, frequency of engagement)
Customer service attributes	segment users by customer service-related attributes (*e.g.*, feedback types such as bugs, suggestions, and help)
Device attributes	characteristics of the device being used to access the TikTok platform (*e.g.,* make, model, OS type, OS version)
Device health statistics	statistics that can be used to check whether the app resource usage is normal (e.g., CPU utilization, memory usage, battery usage)
Digg push off/on	indicates whether a user has turned on system notifications for likes their content receives
E-commerce product attributes	characteristics of an e-commerce product (*e.g.*, product category, price range)
Engineering Shard Group	identifies from which "shards" given data originated (*i.e.,* for systems too large to host in a single machine, the system is split into different shards, each shard handles different parts of data and each shard consists of several processes). This identifier allows the engineering team to identify if there are certain shards/systems that are not meeting performance expectations.
Evaluation metrics	metrics which can be used to evaluate the performance of AI models or other technical optimizations (*e.g.*, network optimization)
Execution attribute	tag for moderation purposes (*e.g.*, pornography, hate speech, language) to facilitate queueing for review
Experiment group	randomized sampling of users, with no identifying information (will only ever be generated by the TTP, with no ByteDance/TikTok insight into identifiable user data)
Flow control	attributes related to a mechanism for controlling how many and how fast advertisements should be delivered to users; there is a module in the advertisements delivery system to enable the mechanism
Follow new story push off/on	indicates whether a user has turned on push notifications for following of new stories
Follow push off/on	indicates whether a user has turned on push notifications for follows

3

APP-519

General statistics	general statistics (*e.g.*, sum, average, standard deviation)
Geo	geographic information (*i.e.,* country, state, county, city, Nielsen designated market area)
Gift attributes	attributes of a live streaming gift, which users in the audience can send to a live streaming host (*e.g.*, gift name, gift price)
Grade level	user's age range
Growth attributes	attributes related to how TikTok has acquired a user (*e.g.*, advertising campaign id, media source, new user status, activation date)
Impression	one measure of users' engagement with the advertisement (*e.g.*, user clicked like, user watch advertisement until completion)
Im push off/on	indicates whether a user has turned on push notifications for instant messages
Inner or out app push	whether a push is an in-app notification or system push notification
IVT	abbreviation for "invalid traffic;" it relates to advertising traffic that has been identified through in-house or third party solutions as highly unlikely to be human-triggered and therefore should not be considered in aggregated reporting for advertisers
Labeling results	video labeling flag by a content moderator (*e.g.*, violation, video not recommended, or pass)
Lift or Lift_study	one measure of the performance of an advertisement (*e.g.*, percentage increase in advertiser conversions attributable to the advertisement)
Live attributes	attributes associated with live streaming activities (*e.g.*, the mode of live streaming: Open Broadcaster Studio (OBS) Studio, live studio)
Live inner push off/on	indicates whether a user has turned on push notifications for live onsite events
Live push off/on	indicates whether a user has turned on push notifications for live offsite events
Media property	advertisement platforms (*e.g.*, Google ads, Facebook ads, Twitter ads)
Mention push off/on	indicates whether a user has turned on push notifications for mentions
Network environment	indicates whether a user is accessing the TikTok platform through a wifi network or a cellular data network; the name and address of the network is not provided
Order attributes	attributes related to a user recharge or refund order for sales via the TikTok platform (*e.g.*, recharge reason, order status)
Order status	indicates whether sales orders via the TikTok platform have been placed, paid, shipped, delivered, returned/refunded, or cancelled
Play event	event of a user playing a video in the application

APP-520

Pbole	indicates whether user and their device information is stored in pBole; pBole is an internal system that is responsible for push-related activities
Pbole pushable	indicates whether user and device information can be pushed through pBole.
Performance event	designation of an event where a user encounters a problem (*e.g.,* delay, lag, crash (used for improvement/optimization purposes))
Placement (settings)	settings that allow advertisers to determine where their ads will be delivered (*e.g.*, TikTok landing page, interspersed in "For You" feed)
Predicted age group	user's age group predicated by AI model
Predicted gender	user's gender predicted by AI model
Prediction model	AI models used to predict what users will like; prediction model performance measurements, commonly referred to as "area under the curve", represents how successful the AI model is
Pricing (settings)	settings that allow advertisers to determine the goal on which they will be charged; the possible values are: 1: cpm (Cost Per Mille); 2: cpc (Cost Per Click); 3: cpt (Cost Per Time); 4: noc (self-operated non-charging); 5: gd (Guaranteed delivery); 6: ocpc (Optimization Cost Per Click); 7: cpa (Cost Per Action); 8: ocpm (Optimization Cost Per Mille); 9: cpv (Cost Per View)
Promoted ad attributes	attributes of the promoted mobile apps (*e.g.*, app name registered in TikTok ads platform, the event type that takes place in the app)
Promoted product	types of advertising products that TikTok provides (*e.g.,* dynamic product ads, coupon ads)
Psort cover	indicates whether the pSort system has user or device information; pSort is an internal system for algorithm-based push notifications
Psort send	indicates whether the pSort systems sends push notifications to a user
Push attributes	attributes of the push notification (*e.g.*, priority level, timeframe)
Push type	type of push notification
PV	abbreviation for "page views"
Query	designation for any specific user search term; to request aggregated results associated with that term (*e.g.,* how many users have searched for "superbowl2020", "charlidamelio", "addisonre", etc. during a specific period)
Reason	designation indicating reason for failure of a backend request (*e.g.,* backend service is not available; invalid request)
Recommend video push off/on	indicates whether a user has turned on push notification for recommended videos

APP-521

Referral sources	website or app that led the user to the TikTok platform (*e.g.,* a user searches for a topic using Google and one of the search result is a link to a TikTok video; "Google" would be the referral source)
Referral user attributes	attributes of users who referred other users (*e.g.,* referral action date, activation channel, activation date of referred user, and other common user attributes such as operating system, state, region)
Rule_id	internal unique id of security control rules
Rule hits	number of positive hits of a specific security control rule
Search attributes	characteristics of search behavior within the TikTok app.(*e.g.,* where within the app the search activity is occurring and the document type clocked after a given search)
Search channel attributes	attributes of users acquired through search channel (*e.g.,* search source, search keyword, if search page has result)
Search scenario	source/channel for the initiation of the search within the TikTok app (*e.g.,* tab at the bottom of the app where the searches can be initiated like "Discover" tab, "Video" tab, and "Music" tab)
Search user type	type of users who performed search (*e.g.,* registered user, unregistered user)
Security attributes	Security attributes refer to security control decisions (e.g., pass, observe and block) and security engineering features (e.g., type of event, past security verdict of account, account signup channel)
Shop	seller/shop that is providing the merchandise (*e.g.,* Nike official)
Shopping process flow	designation for the steps in the in-app shopping process (*e.g.,* viewing, added to cart, review cart, checkout)
Stages of delivery system	internal steps in the ads delivery pipeline (*e.g.,* target setting mapping, regional risk-control, ads frequency control, ads-blocking, ecpm ranking)
Status of followship	user tier by number of followers
Story interaction push off/on	indicates whether a user has turned on push notifications for story interactions
Survey attributes	attributes of the user completed survey (*e.g.,* questionnaire ID, questionnaire name, questionnaire type – long text v. multiple choice)
Tag status & availability	tags for the audience targeting implementation; they indicate the status and availability of the tag generating process
Targeting (settings)	settings that allow advertisers to set to whom they want their ad groups delivered; could be a combination of targeting attributes and their values (*e.g.,* "female 18-24 users who are in NYC")
Targeting attributes	attributes that are associated with a group that the advertiser wants to target (*e.g.,* age range, gender, country and region, device platform)
Tasks	tasks assigned to a content moderator (*e.g.,* labeling a video)

APP-522

Task attributes	attributes of a live streaming task, which the operator can configure in the operation platform (*e.g.*, task name, task time, task config)
Tbase	indicates whether a user device is in Tbase; Tbase is an internal system that stores user device information for content delivery
Ttpush	indicates whether a user or device is in TTPush; TTPush is an internal system for push notifications
Union attributes	attributes of a live streaming union, which is a business organization managing a list of live streaming hosts (*e.g.*, union name, country of a union)
User active history	user's historical engagement with the app (*e.g.*, number of days the user is active in the app)
User attributes	segment users by source (*e.g.*, paid ads, referral, organic); location (*e.g.*, regions, countries, states); behaviors (*e.g.*, lifetime, active date)
User properties	same as "User attributes"
User grouping	same as "User attributes"
User Scenario	designation for the relevant page of the TikTok app (*e.g.,* "For You" feed, profile, search)
UV	abbreviation for "unique visitor" or "unique user"; refers to a person who has visited the website at least once and is counted only once in the reporting time period, even if through multiple sessions
UX performance metrics	user experience performance data (*e.g.,* latency, time to load first video, crash metrics)
Video attributes	designation for certain video characteristics (*e.g.,* video effects, filters, hashtags, music)
Video content attribution	technical attributes of the video content (*e.g.,* height, width, resolution, duration, music, album)

APP-523

Material Under Seal Deleted

Material Under Seal Deleted

Material Under Seal Deleted

Material Under Seal Deleted

Material Under Seal Deleted

Material Under Seal Deleted